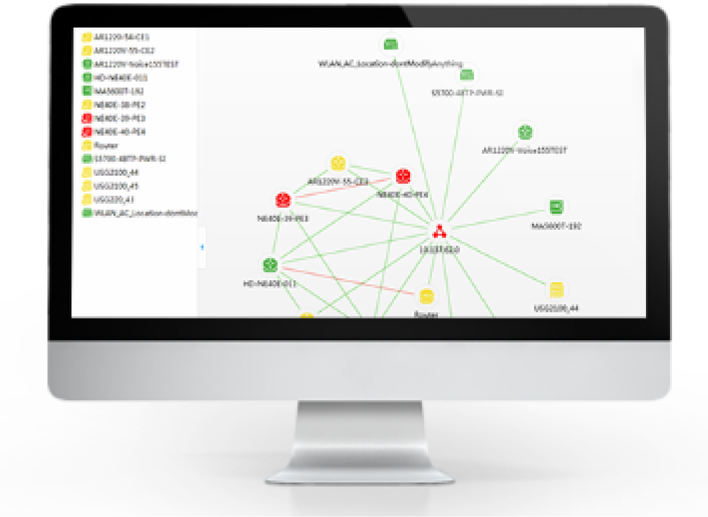
# *Harris Corporation v. Huawei, et al* – Case No. 2:18-cv-439
## Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)
## Exhibit A – U.S. Patent No. 6,535,227 ('227) – Claims 1-6, 8-13, 15-20, 22, 24

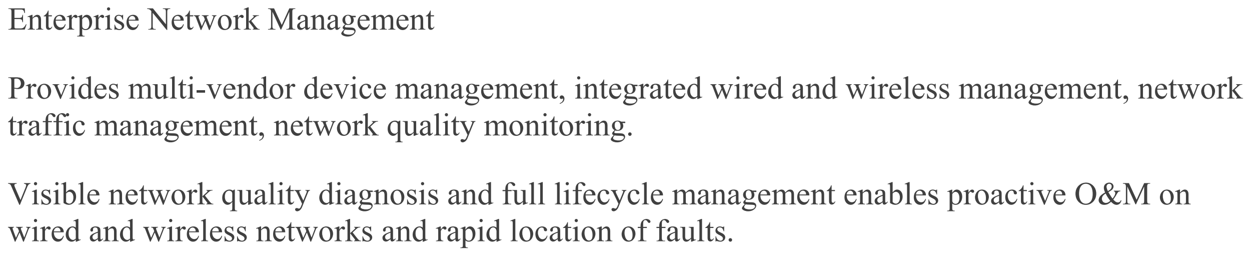
Harris Corporation expressly reserves the right to supplement or modify these Disclosures as appropriate upon receipt of further information and discovery. The Huawei '227 Patent Instrumentalities (as that term is defined and the corresponding devices are identified in Harris's P.R. 3-1 and P.R. 3-2 disclosures cover pleading) infringe at least the following claims. References to instrumentalities in this chart are exemplary only and should not be construed as limiting the scope of any claim of the '227 patent. Further, Huawei documentation referenced below do not identify all the graphical user interface features of the products, and Harris reserves the right to supplement after discovery. The Huawei '227 Patent Accused Instrumentalities satisfy each claim element below literally. The Huawei '227 Patent Accused Instrumentalities also satisfy claim elements under the Doctrine of Equivalents, including without limitation where specifically identified below, because they include and perform substantially similar functionality.

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| **1.** A graphical user interface contained on a computer screen and used for determining the security posture of a network comprising: | The Huawei '227 Patent Accused Instrumentalities infringe this claim.<br>For example, Huawei makes, uses, sells, offers for sale and/or imports the eSight software that creates a graphical user interface on a computer screen that can be used for determining the security posture of a network. eSight may be used to display a graphical user interface on a computer, including, for example, the Huawei Matebook. Huawei further directs its customers to use eSight software and user interface on a variety of computers, browsers and computer screens and specifically intends for users to do so. |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | Critical<br>Major<br>Minor<br>Warning<br>Top N Conversation Traffic<br>Top N Host Traffic<br>Top N DSCP Traffic<br>eSight Platform<br>Supports unified management of storages, servers, applications, switches, routers, firewalls, APs, GPON, eLTE, camera, IP phones, and videoconferencing devices. Provides functions including unified view, resource management, topology, performance, and intelligent configuration for heterogeneous devices. Supports customization of third-party devices and NBI for alarms. These functions constitute a unified management system for customers and ensure lower O&M costs and higher efficiency.<br>https://e.huawei.com/en/products/software |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | eSight Platform<br>Huawei eSight Platform supports unified management of storage devices, servers, applications, switches, routers, firewalls, WLANs, Passive Optical Networks (PONs), wireless broadband trunk devices, video surveillance devices, IP phones, and videoconferencing devices. eSight provides functions including unified view, resource management, topology, performance, and intelligent configuration for heterogeneous devices. eSight also supports customization of third-party devices and NBI for alarms. These functions constitute a unified management system for customers and ensure lower O&M costs and higher efficiency.<br>https://e.huawei.com/en/products/software/mgmt-sys/esight/esight-platform<br> AR1220-5A-CE1<br>AR1220V-5S-CE2<br>AR1220V-Voice155TEST<br>HD-NE40E-011<br>MA5600T-192<br>NE40E-38-PE2<br>NE40E-39-PE3<br>NE40E-40-PE4<br>Router<br>S5700-48TP-PWR-SI<br>USG2100_44<br>USG2100_45<br>USG220_41<br>WLAN_AC_location-dontModifyAnything<br>S5700-48TP-PWR-SI<br>AR1220V-Voice155TEST<br>AR1220V-5S-CE2<br>NE40E-40-PE4<br>NE40E-39-PE3<br>MA5600T-192<br>HD-NE40E-011<br>Router<br>USG2100_44 |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|

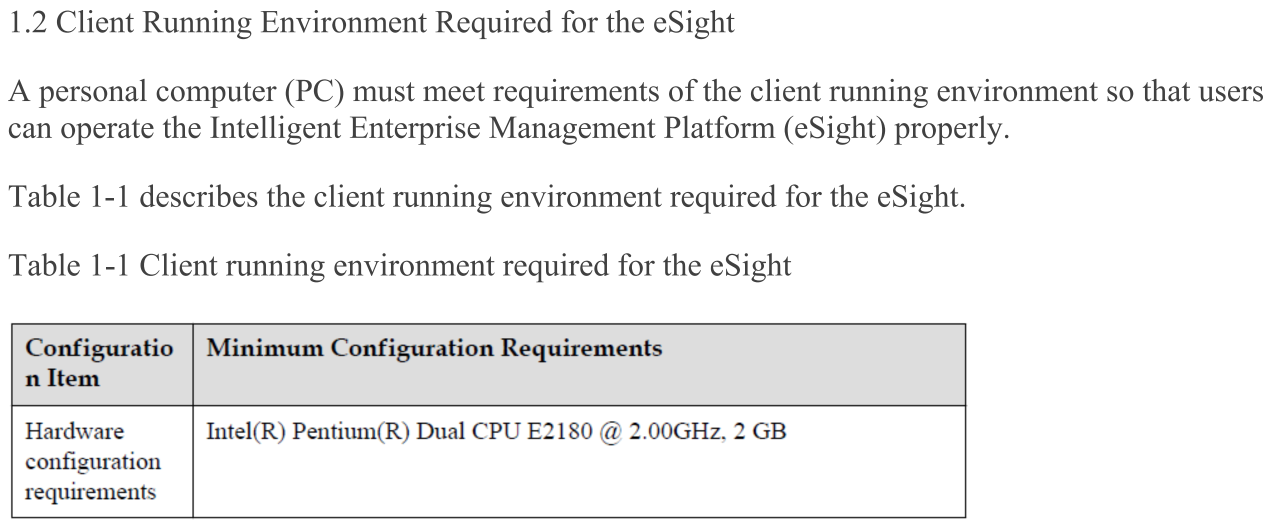


Enterprise Network Management

Provides multi-vendor device management, integrated wired and wireless management, network traffic management, network quality monitoring.

Visible network quality diagnosis and full lifecycle management enables proactive O&M on wired and wireless networks and rapid location of faults.

https://e.huawei.com/en/products/software; *see also* https://e.huawei.com/en/products/software/mgmt-sys/esight/network-management (Enterprise Network Management is part of eSight family)



1.2 Client Running Environment Required for the eSight

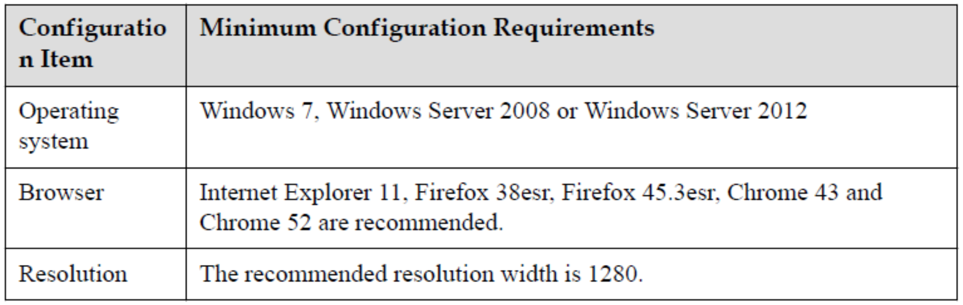
A personal computer (PC) must meet requirements of the client running environment so that users can operate the Intelligent Enterprise Management Platform (eSight) properly.

Table 1-1 describes the client running environment required for the eSight.

Table 1-1 Client running environment required for the eSight

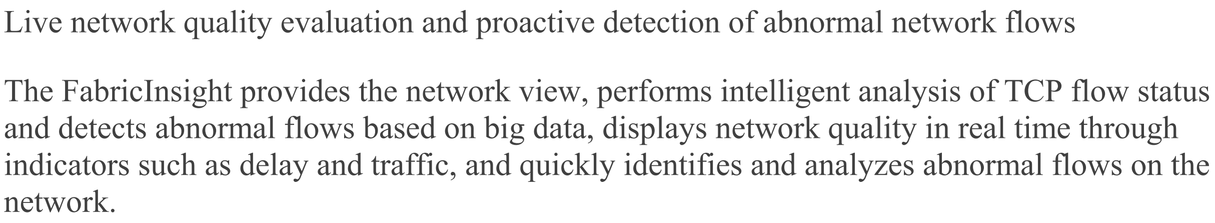
| Configuration Item | Minimum Configuration Requirements |
|---|---|
| Hardware configuration requirements | Intel(R) Pentium(R) Dual CPU E2180 @ 2.00GHz, 2 GB |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | |



| Configuration Item | Minimum Configuration Requirements |
|---|---|
| Operating system | Windows 7, Windows Server 2008 or Windows Server 2012 |
| Browser | Internet Explorer 11, Firefox 38esr, Firefox 45.3esr, Chrome 43 and Chrome 52 are recommended. |
| Resolution | The recommended resolution width is 1280. |

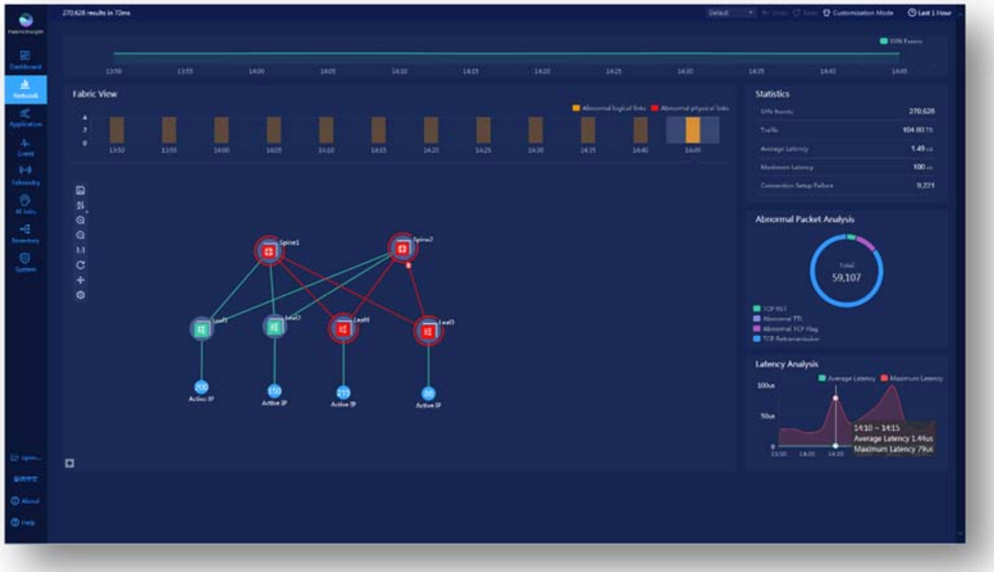
Further, Huawei makes, uses, sells, offers to sell and/or imports the FabricInsight software that creates a graphical user interface on a computer screen that can be used for determining the security posture of a network. For example:



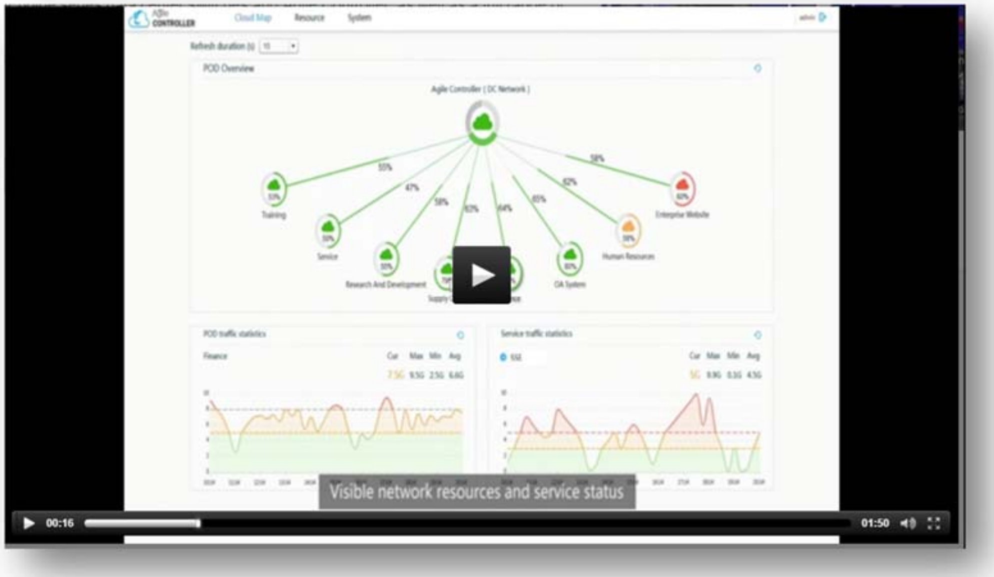
Live network quality evaluation and proactive detection of abnormal network flows

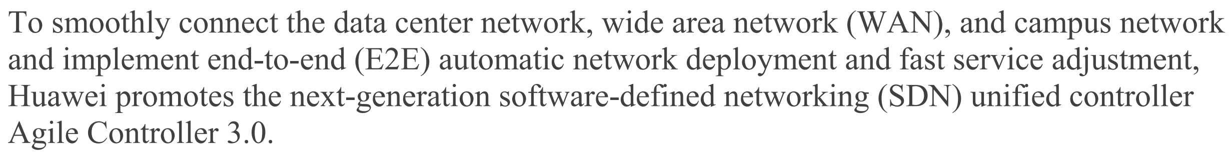
The FabricInsight provides the network view, performs intelligent analysis of TCP flow status and detects abnormal flows based on big data, displays network quality in real time through indicators such as delay and traffic, and quickly identifies and analyzes abnormal flows on the network.

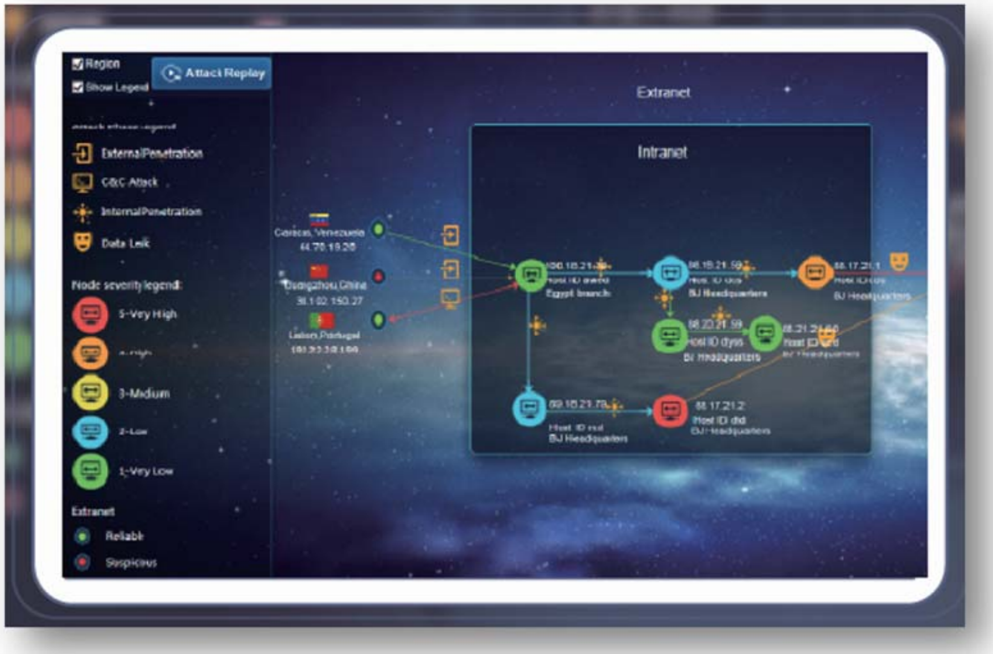
*Harris Corporation v. Huawei, et al* – Case No. 2:18-cv-439
Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)
Exhibit A – U.S. Patent No. 6,535,227 ('227) – Claims 1-6, 8-13, 15-20, 22, 24

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |   Fabric View<br>Statistics<br>270,626<br>1.49<br>100<br>9,221<br>Abnormal Packet Analysis<br>Total<br>59,107<br>Latency Analysis<br>100us<br>50us<br>14:10 ~ 14:15<br>Average Latency 1.44us<br>Maximum Latency 79us<br>Spine1<br>Spine2<br>Leaf1<br>Leaf2<br>Leaf3<br>200<br>150<br>215<br>Active IP<br>Dashboard<br>Network<br>Application<br>About<br>Help<br>Huawei FabricInsight Datasheet at 4.<br>Further, Huawei makes, uses, sells, offers to sell and/or imports software used in SDN or Software Defined Networks, including the Agile Controller software that creates a graphical user interface on a computer screen that can be used for determining the security posture of a network. For example: |

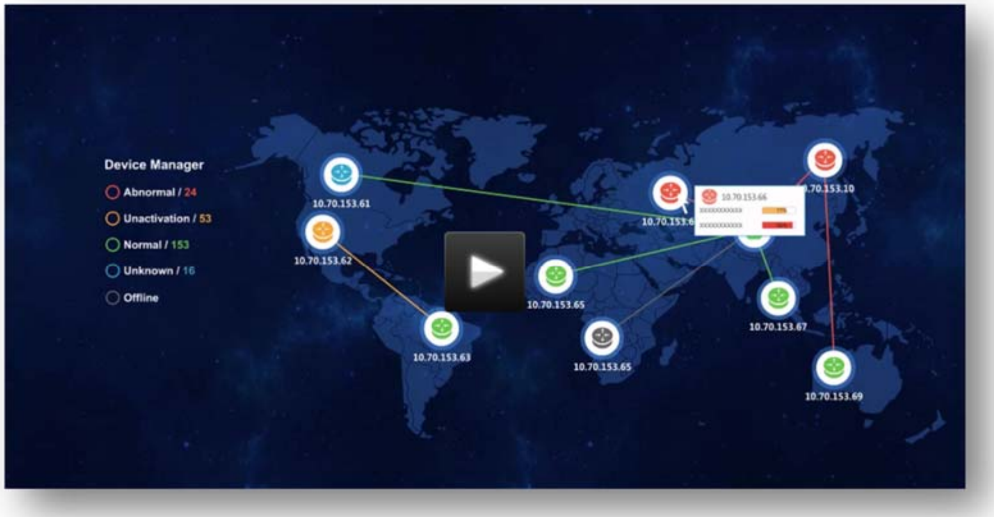
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | <br> https://e.huawei.com/en/products/enterprise-networking/sdn-controller/agile-controller/wan |

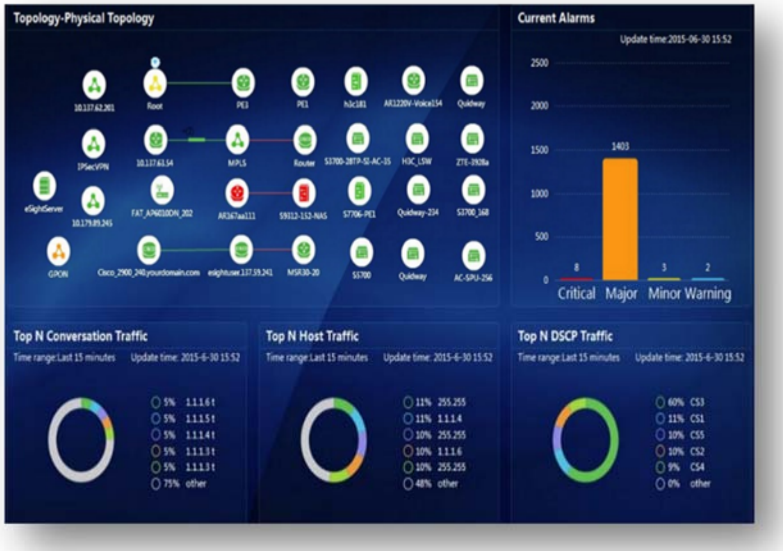
| **'227 PATENT CLAIM 1** | **INFRINGEMENT BY HUAWEI CORPORATION** |
|---|---|
| | *See also*:<br><br> Agile CONTROLLER<br>Cloud Map<br>Resource<br>System<br>admin<br>Refresh duration (s) 15<br>POD Overview<br>Agile Controller ( DC Network )<br>55%<br>47%<br>58%<br>63%<br>64%<br>65%<br>62%<br>58%<br>Training<br>Service<br>Research And Development<br>Supply<br>OA System<br>Human Resources<br>Enterprise Website<br>POD traffic statistics<br>Finance<br>Cur Max Min Avg<br>7.5G 9.5G 2.5G 6.6G<br>Service traffic statistics<br>Cur Max Min Avg<br>5G 8.9G 0.3G 4.5G<br>Visible network resources and service status<br>00:16<br>01:50<br>Huawei Video: *Cloud Fabric: Huawei and VMWare Innovate* (e.huawei.com/en-US/videos/global/older/hw_362493) (Huawei and VMWare co-operate on an SDN data center networking solution) at 0:16. |

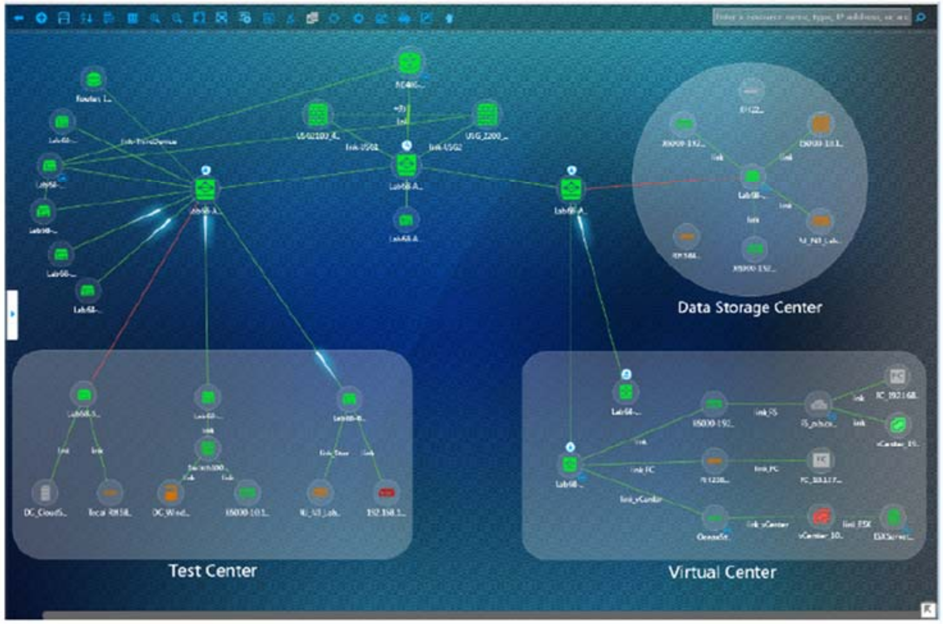
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |  To smoothly connect the data center network, wide area network (WAN), and campus network and implement end-to-end (E2E) automatic network deployment and fast service adjustment, Huawei promotes the next-generation software-defined networking (SDN) unified controller Agile Controller 3.0.<br>Huawei Agile Controller 3.0 Brief Brochure V1.0 at 1.<br>Further, Huawei makes, uses, sells, offers to sell and/or imports software used in SDN or Software Defined Networks, including the Cybersecurity Intelligence System (CIS) software that creates a graphical user interface on a computer screen that can be used for determining the security posture of a network. |

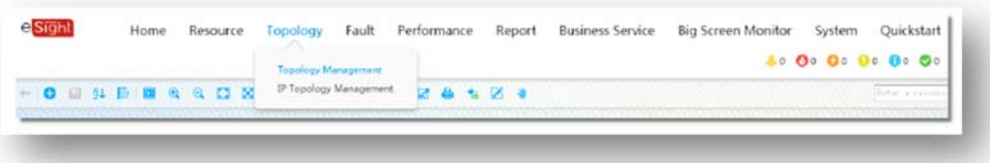
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |  Region<br>Show Legend<br>Attack Replay<br>ExternalPenetration<br>C&C Attack<br>InternalPenetration<br>Data Leik<br>Node severity legend:<br>5-Very High<br>3-Medium<br>2-Low<br>1-Very Low<br>Extranet<br>Reliable<br>Suspicious<br>Extranet<br>Intranet<br>Caracas, Venezuela<br>Guangzhou China<br>Lisbon, Portugal<br>Egypt branch<br>BJ Headquarters<br>Host ID dyss<br>Host ID did<br>Display of Security Posture on the Network Topology<br>The security posture awareness function maps network security threat events to a global topological map, uses the threat map to display threats and lately discovered threat events, and predicts and alerts the trend of network security.<br>Huawei CIS Cybersecurity Intelligence System Product Description at 3. |

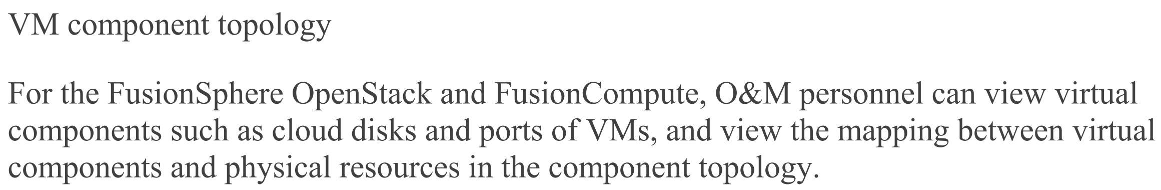
| **'227 PATENT CLAIM 1** | **INFRINGEMENT BY HUAWEI CORPORATION** |
|---|---|
| **[a]** a system design window for displaying network icons of a network map that are representative of different network elements contained within a network, wherein respective network icons are linked together in an arrangement corresponding to how network elements are interconnected within the network; | The graphical user interface of the '227 Patent Accused Instrumentalities comprises a system design window for displaying network icons of a network map that are representative of different network elements contained within a network, wherein respective network icons are linked together in an arrangement corresponding to how network elements are interconnected within the network.<br>For example, the eSight topology view window allows for displaying network icons that are representative of different network elements (for example, routers, gateways, Wireless Area Network (WLAN) devices, UC devices, video surveillance devices, and telepresence devices) that are linked in an arrangement corresponding to how network elements are interconnected. For example:<br>"Topology view displays the entire network topology and real time statuses of devices and links. One look at the topology view provides you with an overview of the entire network. Clicking on a device in the topology view allows you to learn about its running status and alarms." |

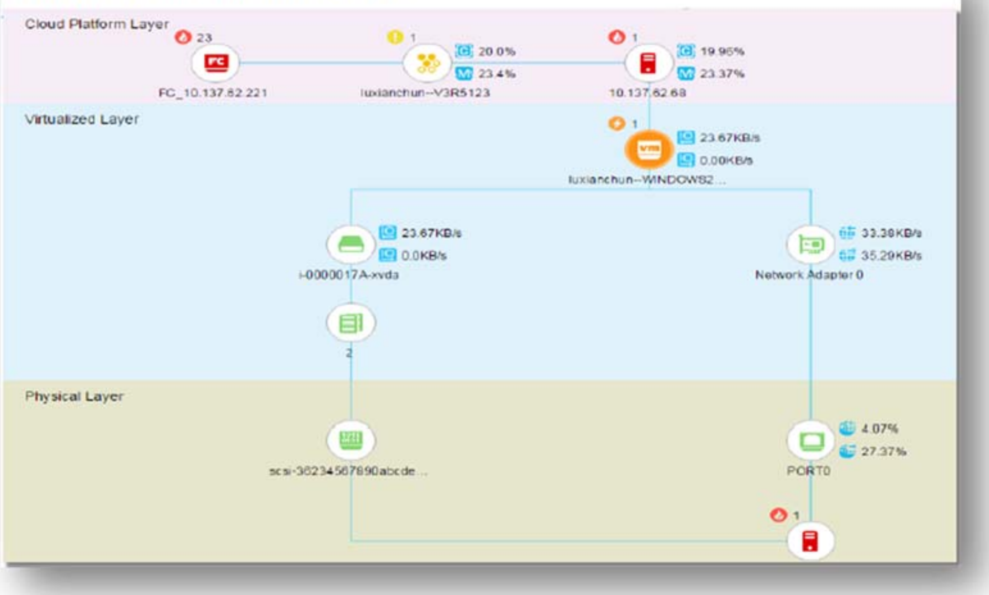
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |  Device Manager<br>○ Abnormal / 24<br>○ Unactivation / 53<br>○ Normal / 153<br>○ Unknown / 16<br>○ Offline<br>10.70.153.61<br>10.70.153.62<br>10.70.153.63<br>10.70.153.65<br>10.70.153.65<br>10.70.153.6<br>10.70.153.66<br>.70.153.10<br>10.70.153.67<br>10.70.153.69<br>Unified View video at 0:30 https://e.huawei.com/en/products/software/mgmt-sys/esight/esight-platform |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | <br> Topology-Physical Topology<br>10.137.62.201<br>Root<br>PE3<br>PE1<br>h3c181<br>AR1220V-Voice154<br>Quidway<br>IPSecVPN<br>10.137.61.54<br>MPLS<br>Router<br>S3700-28TP-SI-AC-15<br>H3C_LSW<br>ZTE-2928a<br>eSightServer<br>10.179.89.245<br>FAT_AP6010DN_202<br>AR167aa111<br>S9312-152-NAS<br>S7706-PE1<br>Quidway-234<br>S3700_168<br>GPON<br>Cisco_2900_240.yourdomain.com<br>eightuser.137.59.241<br>MSR30-20<br>S5700<br>Quidway<br>AC-SPU-256<br>Current Alarms<br>Update time:2015-06-30 15:52<br>2500<br>2000<br>1500<br>1000<br>500<br>0<br>8<br>1403<br>3<br>2<br>Critical<br>Major<br>Minor<br>Warning<br>Top N Conversation Traffic<br>Time range:Last 15 minutes<br>Update time: 2015-6-30 15:52<br>5% 1.1.1.6 t<br>5% 1.1.1.5 t<br>5% 1.1.1.4 t<br>5% 1.1.1.3 t<br>5% 1.1.1.3 t<br>75% other<br>Top N Host Traffic<br>Time range:Last 15 minutes<br>Update time: 2015-6-30 15:52<br>11% 255.255<br>11% 1.1.1.4<br>10% 255.255<br>10% 1.1.1.6<br>10% 255.255<br>48% other<br>Top N DSCP Traffic<br>Time range:Last 15 minutes<br>Update time: 2015-6-30 15:52<br>60% CS3<br>11% CS1<br>10% CS5<br>10% CS2<br>9% CS4<br>0% other<br>https://e.huawei.com/en/products/software/mgmt-sys/esight/esight-platform |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | Figure 7-1 shows the GUI of topology management.<br>**Figure 7-1** GUI of topology management<br><br> <br>eSight Operations Guide Issue 08 (2018-08-28) at 295. |

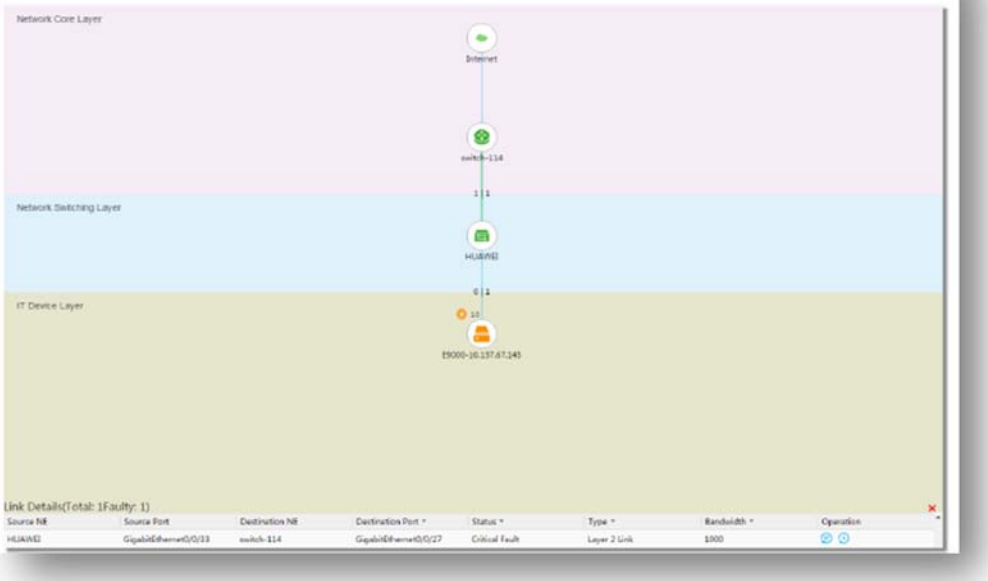
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | As the eSight guide further explains in Setting up the Physical Topology:<br>Step 1 Obtain the completed network design.<br>A network is divided by following certain principles. For example:<br>• By the area where devices are located<br>• By device type<br>• By device Internet Protocol (IP) address<br>• By device owner<br>Step 2 Choose Topology > Topology Management from the main menu.<br> eSight<br>Home<br>Resource<br>Topology<br>Fault<br>Performance<br>Report<br>Business Service<br>Big Screen Monitor<br>System<br>Quickstart<br>Topology Management<br>IP Topology Management<br>Step 3 Arrange topology objects based on the network design. Then click to save their new positions after the adjustment.<br>eSight Operations Guide Issue 08 (2018-08-28) at 296. |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | This claim limitation is further met when virtual network mapping occurs, for example, through software defined networking (SDN). For example, eSight Virtual Resources Manager further allows for the display of virtual component topology:<br><br>VM component topology<br>For the FusionSphere OpenStack and FusionCompute, O&M personnel can view virtual components such as cloud disks and ports of VMs, and view the mapping between virtual components and physical resources in the component topology. |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | **Figure 11-4** VM component topology<br> Cloud Platform Layer<br>23<br>FC_10.137.62.221<br>1<br>20.0%<br>23.4%<br>luxianchun--V3R5123<br>1<br>19.96%<br>23.37%<br>10.137.62.68<br>Virtualized Layer<br>1<br>23.67KB/s<br>0.00KB/s<br>luxianchun--WINDOWS2...<br>23.67KB/s<br>0.0KB/s<br>i-0000017A-xvda<br>33.39KB/s<br>35.29KB/s<br>Network Adapter 0<br>2<br>Physical Layer<br>scsi-36234567890abcde...<br>4.07%<br>27.37%<br>PORT0<br>1<br>VM physical topology<br>For the FusionSphere OpenStack and FusionCompute, O&M personnel can view the network topology from the physical device where the VM is located to the external routers from the VM perspective. |

<table>
<tr><th>'227 PATENT CLAIM 1</th><th>INFRINGEMENT BY HUAWEI CORPORATION</th></tr>
<tr><td></td><td>

**Figure 11-5** VM physical topology



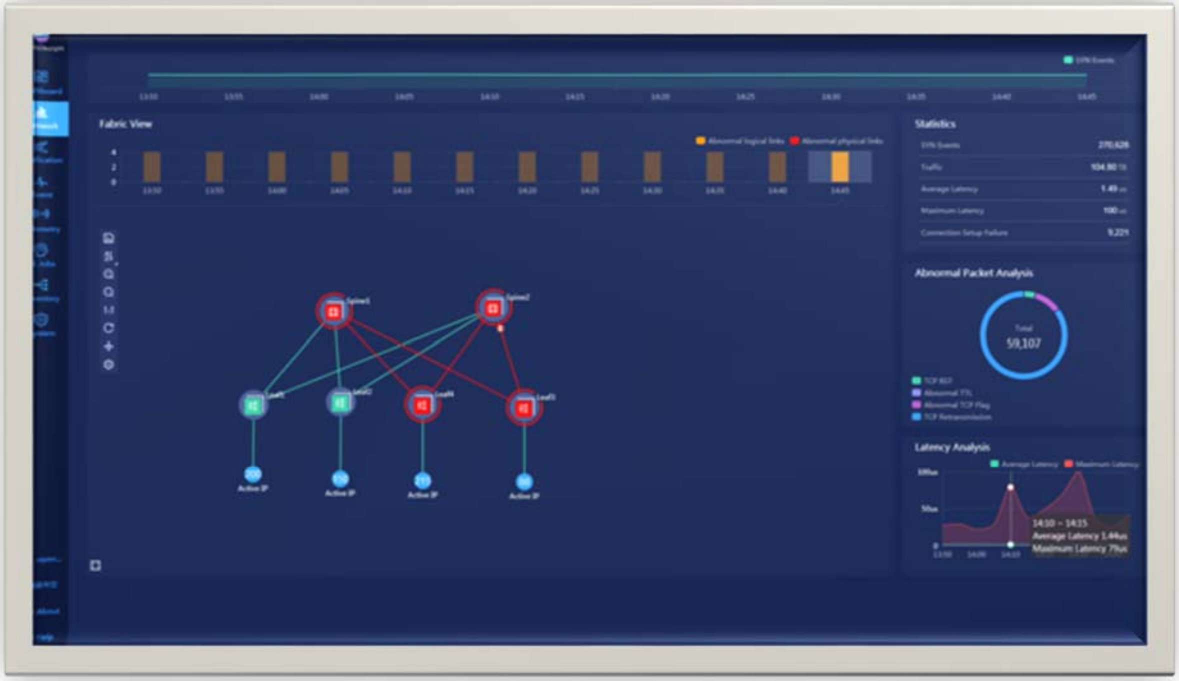
Link Details(Total: 1Faulty: 1)

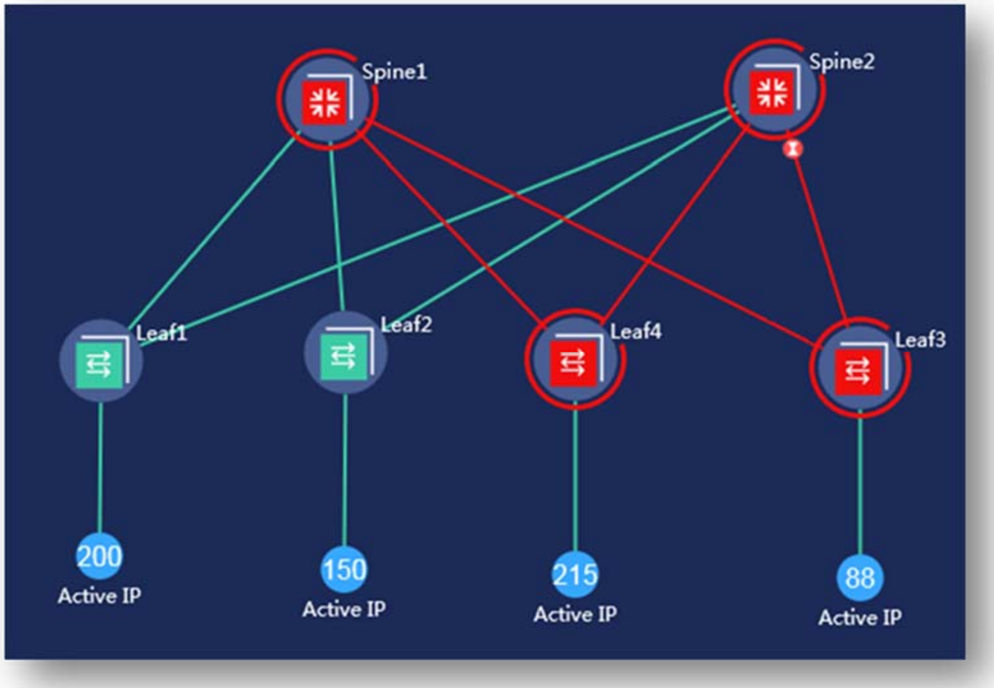
| Source NE | Source Port | Destination NE | Destination Port | Status | Type | Bandwidth | Operation |
|---|---|---|---|---|---|---|---|
| HUAWEI | GigabitEthernet0/0/33 | switch-114 | GigabitEthernet0/0/27 | Critical Fault | Layer 2 Link | 1000 | |

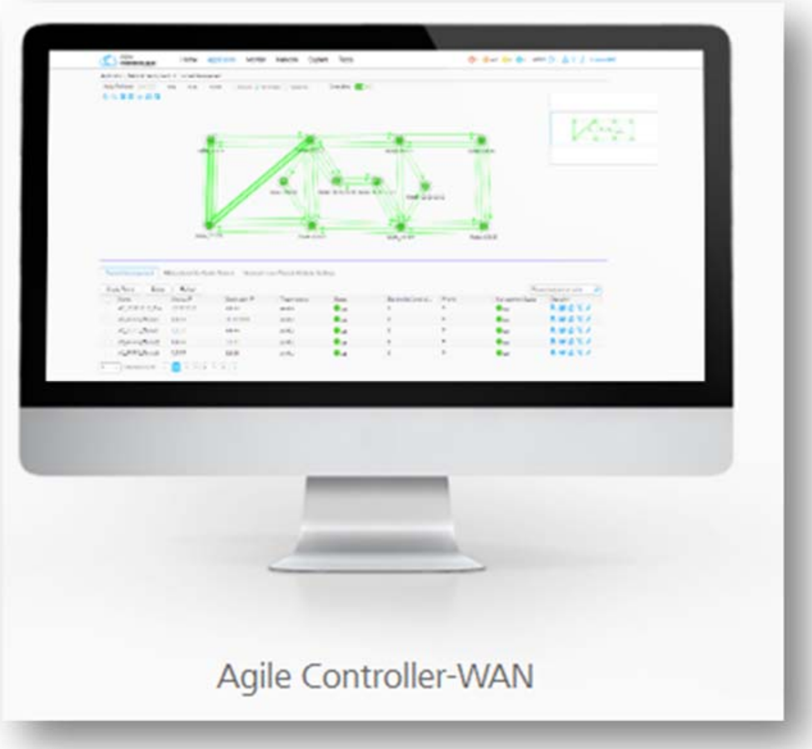
eSight Operations Guide Issue 08 (2018-08-28) at 943-944.

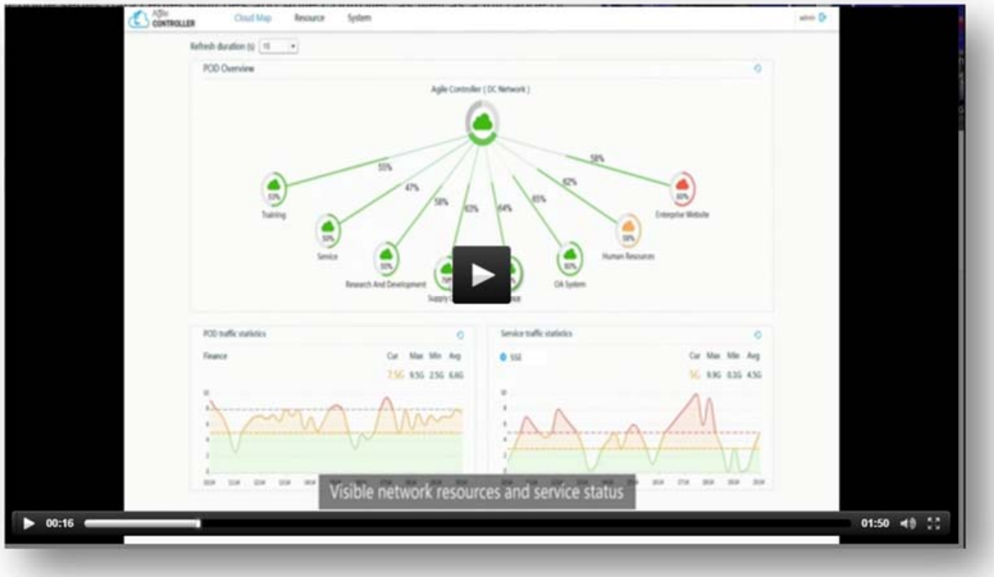
Further, the FabricInsights interface comprises a system design window for displaying network icons of a network map that are representative of different network elements contained within a network, wherein respective network icons are linked together in an arrangement corresponding to how network elements are interconnected within the network

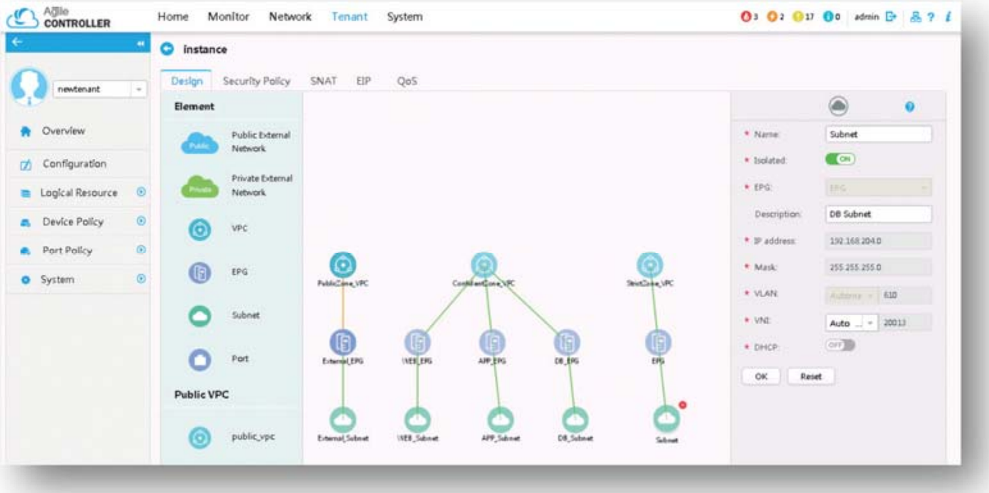
</td></tr>
</table>

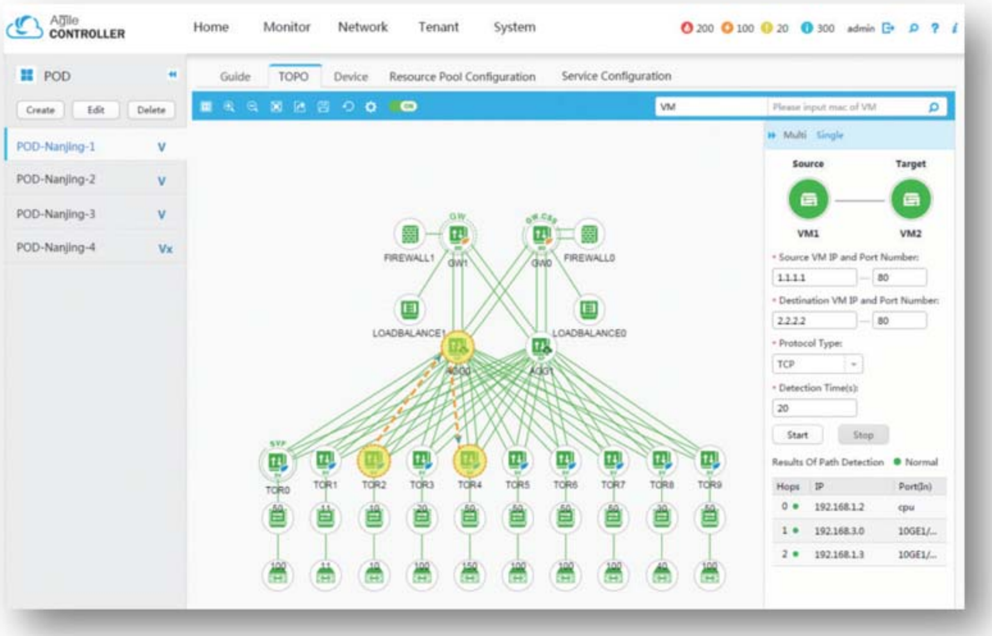
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | Live network quality evaluation and proactive detection of abnormal network flows<br>The FabricInsight provides the network view, performs intelligent analysis of TCP flow status and detects abnormal flows based on big data, displays network quality in real time through indicators such as delay and traffic, and quickly identifies and analyzes abnormal flows on the network.<br><br>Statistics<br>SYN Events 270,628<br>Traffic 104.90 TB<br>Average Latency 1.49 us<br>Maximum Latency 100 us<br>Connection Setup Failure 9,229<br>14:10 – 14:15<br>Average Latency 1.44us<br>Maximum Latency 79us |

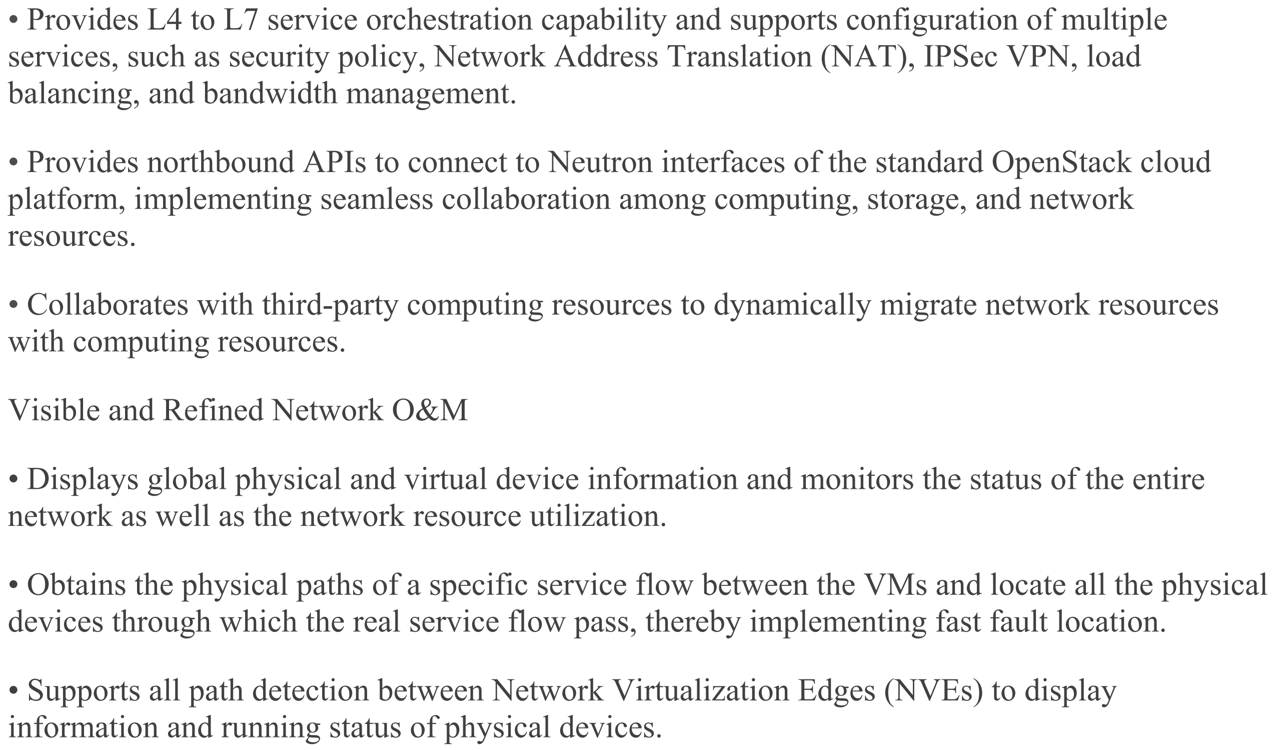
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | <br> Spine1<br>Spine2<br>Leaf1<br>Leaf2<br>Leaf4<br>Leaf3<br>200 Active IP<br>150 Active IP<br>215 Active IP<br>88 Active IP<br>Huawei FabricInsight Datasheet at 3-4.<br>Network visualization [feature]…Displays the Fabric network topology, marks abnormal links, and collects statistics on the number of active IP addresses or leaf switches |

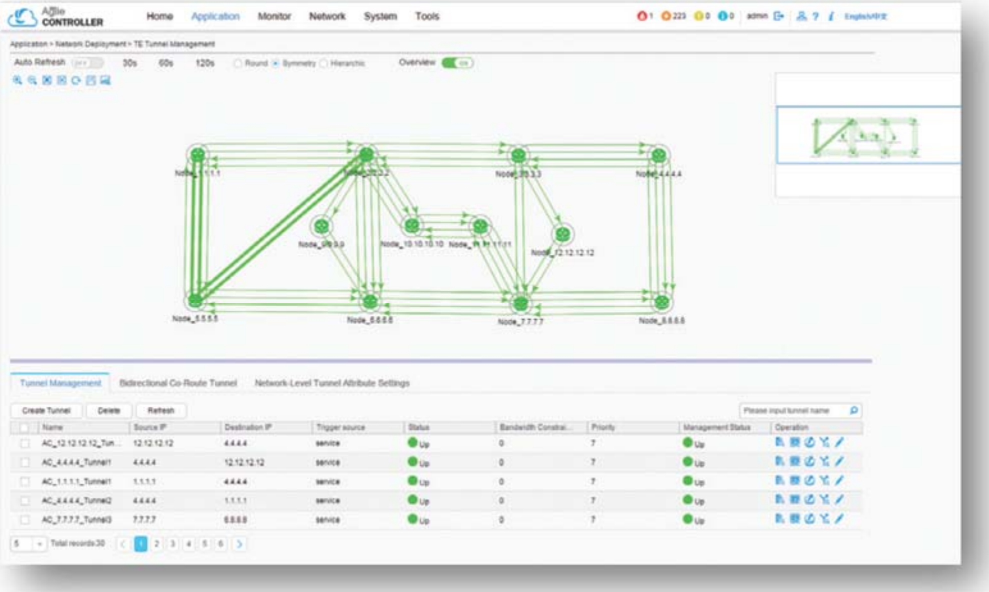
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
|  | Huawei FabricInsight Datasheet at 9.<br>The Agile Controller user interface comprises a system design window for displaying network icons of a network map that are representative of different network elements contained within a network, wherein respective network icons are linked together in an arrangement corresponding to how network elements are interconnected within the network. For example:<br><br> |

| '227 Patent Claim 1 | Infringement By Huawei Corporation |
|---|---|
| | https://e.huawei.com/en/products/enterprise-networking/sdn-controller/agile-controller/wan <br>  <br>  Agile CONTROLLER<br>Cloud Map<br>Resource<br>System<br>admin<br>Refresh duration (s)<br>15<br>POD Overview<br>Agile Controller ( DC Network )<br>55%<br>47%<br>58%<br>63%<br>64%<br>65%<br>62%<br>58%<br>Training<br>Service<br>Research And Development<br>OA System<br>Human Resources<br>Enterprise Website<br>POD traffic statistics<br>Finance<br>Cur<br>Max<br>Min<br>Avg<br>7.5G<br>9.5G<br>2.5G<br>6.6G<br>Service traffic statistics<br>SSE<br>Cur<br>Max<br>Min<br>Avg<br>5G<br>9.9G<br>0.3G<br>4.5G<br>00:16<br>01:50 <br> Visible network resources and service status <br> Huawei Video: *Cloud Fabric: Huawei and VMWare Innovate* (e.huawei.com/en-US/videos/global/older/hw_362493) (Huawei and VMWare co-operate on an SDN data center networking solution) at 0:16. |

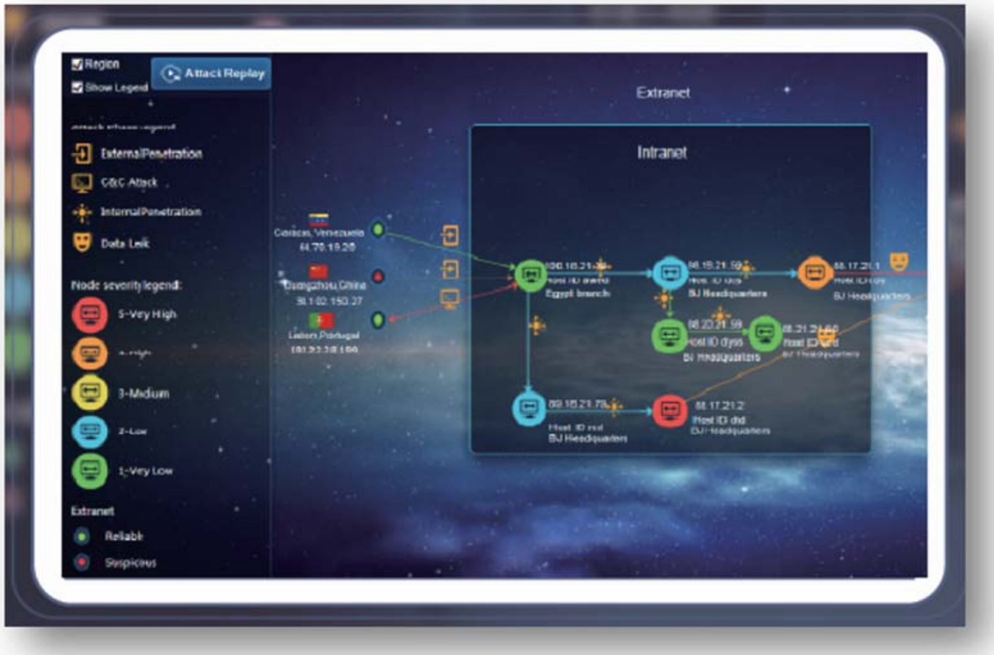
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | <br> Agile CONTROLLER<br>Home<br>Monitor<br>Network<br>Tenant<br>System<br>3<br>2<br>17<br>0<br>admin<br>instance<br>newtenant<br>Overview<br>Configuration<br>Logical Resource<br>Device Policy<br>Port Policy<br>System<br>Design<br>Security Policy<br>SNAT<br>EIP<br>QoS<br>Element<br>Public External Network<br>Private External Network<br>VPC<br>EPG<br>Subnet<br>Port<br>Public VPC<br>public_vpc<br>PublicZone_VPC<br>ConfidentZone_VPC<br>StrictZone_VPC<br>External_EPG<br>WEB_EPG<br>APP_EPG<br>DB_EPG<br>EPG<br>External_Subnet<br>WEB_Subnet<br>APP_Subnet<br>DB_Subnet<br>Subnet<br>OK<br>Reset<br>* Name: Subnet<br>* Isolated: ON<br>* EPG: EPG<br>Description: DB Subnet<br>* IP address: 192.168.204.0<br>* Mask: 255.255.255.0<br>* VLAN: Automa 610<br>* VNI: Auto ... 20013<br>* DHCP: OFF |

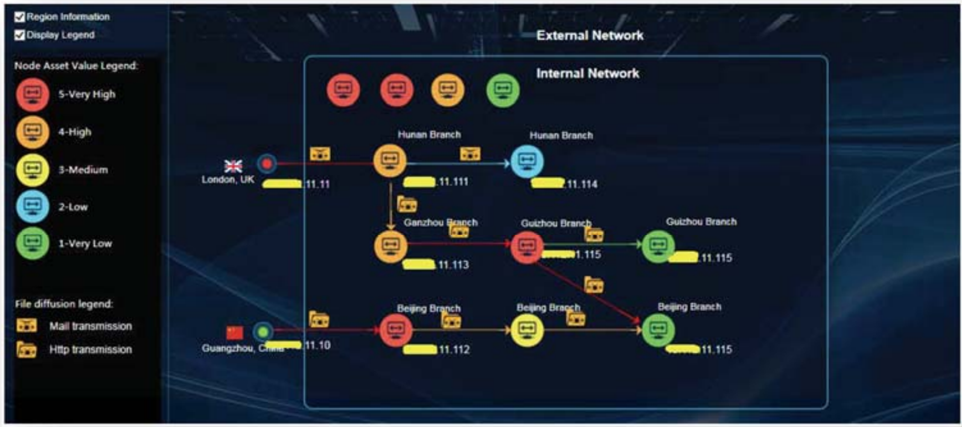
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | <br> Agile CONTROLLER<br>Home<br>Monitor<br>Network<br>Tenant<br>System<br>200<br>100<br>20<br>300<br>admin<br>POD<br>Create<br>Edit<br>Delete<br>POD-Nanjing-1<br>POD-Nanjing-2<br>POD-Nanjing-3<br>POD-Nanjing-4<br>Guide<br>TOPO<br>Device<br>Resource Pool Configuration<br>Service Configuration<br>VM<br>Please input mac of VM<br>Multi<br>Single<br>FIREWALL1<br>GW1<br>GW0<br>FIREWALL0<br>LOADBALANCE1<br>LOADBALANCE0<br>AGG0<br>AGG1<br>TOR0<br>TOR1<br>TOR2<br>TOR3<br>TOR4<br>TOR5<br>TOR6<br>TOR7<br>TOR8<br>TOR9<br>Source VM1 — Target VM2<br>• Source VM IP and Port Number: 1.1.1.1 — 80<br>• Destination VM IP and Port Number: 2.2.2.2 — 80<br>• Protocol Type: TCP<br>• Detection Time(s): 20<br>Start Stop<br>Results Of Path Detection ● Normal<br>Hops / IP / Port(In)<br>0 ● 192.168.1.2 cpu<br>1 ● 192.168.3.0 10GE1/...<br>2 ● 192.168.1.3 10GE1/...<br><br>Automatic Network Deployment and Dynamic Orchestration<br><br>• Defines a network model that allows for drag-and-drop operations on graphical user interfaces (GUIs) in what you see is what get (WYSIWYG) mode. |

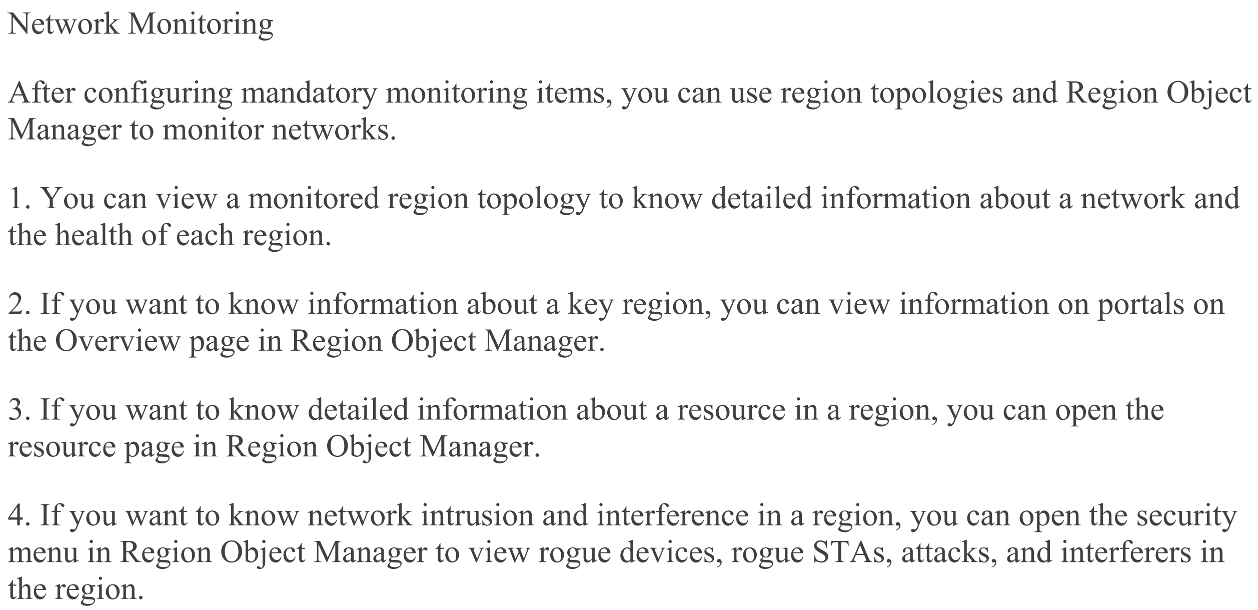
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
|  | <br>• Provides L4 to L7 service orchestration capability and supports configuration of multiple services, such as security policy, Network Address Translation (NAT), IPSec VPN, load balancing, and bandwidth management.<br>• Provides northbound APIs to connect to Neutron interfaces of the standard OpenStack cloud platform, implementing seamless collaboration among computing, storage, and network resources.<br>• Collaborates with third-party computing resources to dynamically migrate network resources with computing resources.<br>Visible and Refined Network O&M<br>• Displays global physical and virtual device information and monitors the status of the entire network as well as the network resource utilization.<br>• Obtains the physical paths of a specific service flow between the VMs and locate all the physical devices through which the real service flow pass, thereby implementing fast fault location.<br>• Supports all path detection between Network Virtualization Edges (NVEs) to display information and running status of physical devices.<br>Huawei Agile Controller 3.0 Brief Brochure V1.0 at 2. |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |  Agile CONTROLLER<br>Home<br>Application<br>Monitor<br>Network<br>System<br>Tools<br>1<br>223<br>0<br>0<br>admin<br>English/中文<br>Auto Refresh<br>30s<br>60s<br>120s<br>Round<br>Symmetry<br>Hierarchic<br>Overview<br>Node_1.1.1.1<br>Node_2.2.2.2<br>Node_3.3.3.3<br>Node_4.4.4.4<br>Node_9.9.9.9<br>Node_10.10.10.10<br>Node_11.11.11.11<br>Node_12.12.12.12<br>Node_5.5.5.5<br>Node_6.6.6.6<br>Node_7.7.7.7<br>Node_8.8.8.8<br>Tunnel Management<br>Bidirectional Co-Route Tunnel<br>Network-Level Tunnel Attribute Settings<br>Create Tunnel<br>Delete<br>Refresh<br>Please input tunnel name<br>Application > Network Deployment > TE Tunnel Management<br>□ Name \| Source IP \| Destination IP \| Trigger source \| Status \| Bandwidth Constrai... \| Priority \| Management Status \| Operation<br>□ AC_12.12.12.12_Tun... \| 12.12.12.12 \| 4.4.4.4 \| service \| ● Up \| 0 \| 7 \| ● Up<br>□ AC_4.4.4.4_Tunnel1 \| 4.4.4.4 \| 12.12.12.12 \| service \| ● Up \| 0 \| 7 \| ● Up<br>□ AC_1.1.1.1_Tunnel1 \| 1.1.1.1 \| 4.4.4.4 \| service \| ● Up \| 0 \| 7 \| ● Up<br>□ AC_4.4.4.4_Tunnel2 \| 4.4.4.4 \| 1.1.1.1 \| service \| ● Up \| 0 \| 7 \| ● Up<br>□ AC_7.7.7.7_Tunnel3 \| 7.7.7.7 \| 8.8.8.8 \| service \| ● Up \| 0 \| 7 \| ● Up<br>5 Total records:30 < 1 2 3 4 5 6 ><br><br>Topology Management<br><br>• Supports collecting physical and logical network topology information and displays network-wide topology:<br><br>Huawei Agile Controller 3.0 Brief Brochure V1.0 at 3.<br><br>Further, the CIS user interface comprises a system design window for displaying network icons of a network map that are representative of different network elements contained within a network, wherein respective network icons |

*Harris Corporation v. Huawei, et al* – **Case No. 2:18-cv-439**
**Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)**
**Exhibit A – U.S. Patent No. 6,535,227 ('227) – Claims 1-6, 8-13, 15-20, 22, 24**

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | are linked together in an arrangement corresponding to how network elements are interconnected within the network. For example:<br> Region<br>Show Legend<br>Attack Replay<br>ExternalPenetration<br>C&C Attack<br>InternalPenetration<br>Data Leik<br>Node severity legend:<br>5-Very High<br>3-Midium<br>2-Low<br>1-Very Low<br>Extranet<br>Reliable<br>Suspicious<br>Extranet<br>Intranet<br>Caracas, Venezuela<br>44.70.19.20<br>Guangzhou China<br>58.1.02.150.27<br>Lisbon Portugal<br>Egypt branch<br>88.15.21.59<br>BJ Headquarters<br>88.17.21.1<br>BJ Headquarters<br>88.23.21.59<br>Host ID dyss<br>BJ Headquarters<br>89.18.21.78<br>BJ Headquarters<br>88.17.21.2<br>Host ID did<br>Display of Security Posture on the Network Topology<br>The security posture awareness function maps network security threat events to a global topological map, uses the threat map to display threats and lately discovered threat events, and predicts and alerts the trend of network security. |

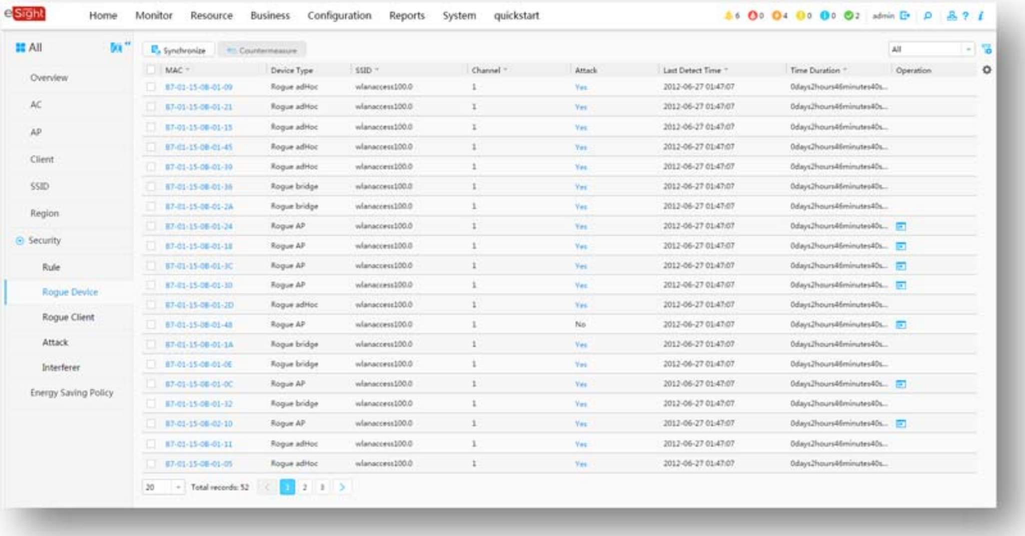
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | Huawei CIS Cybersecurity Intelligence System Product Description at 3.<br>*See also, e.g.,*:<br> ☑ Region Information<br>☑ Display Legend<br>Node Asset Value Legend:<br>5-Very High<br>4-High<br>3-Medium<br>2-Low<br>1-Very Low<br>File diffusion legend:<br>Mail transmission<br>Http transmission<br>External Network<br>Internal Network<br>London, UK<br>11.11<br>Hunan Branch<br>11.111<br>Hunan Branch<br>11.114<br>Ganzhou Branch<br>11.113<br>Guizhou Branch<br>1.115<br>Guizhou Branch<br>11.115<br>Guangzhou, China<br>11.10<br>Beijing Branch<br>11.112<br>Beijing Branch<br>Beijing Branch<br>11.115<br>Huawei CIS Cybersecurity Intelligence System Datasheet at 4. |
| **[b]** wherein selected portions of the network map turn a different color indicative of a vulnerability that has been established for | The graphical user interface of the '227 Patent Accused Instrumentalities further comprises the capability for selected portions of the network map to turn a different color indicative of a vulnerability that has been established for that portion of the network after a security posture of the network has been established by correlating a system object model database that supports information data requirements of disparate network vulnerability analysis programs with any data results obtained from the programs. |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| that portion of the network after a security posture of the network has been established by correlating a system object model database that supports information data requirements of disparate network vulnerability analysis programs with any data results obtained from the programs. | For example, eSight region topologies and Region Object Manager allow for the identification of vulnerabilities, including, without limitation, rogue devices, rogue STAs, attacks, and interferers:<br><br>Network Monitoring<br>After configuring mandatory monitoring items, you can use region topologies and Region Object Manager to monitor networks.<br>1. You can view a monitored region topology to know detailed information about a network and the health of each region.<br>2. If you want to know information about a key region, you can view information on portals on the Overview page in Region Object Manager.<br>3. If you want to know detailed information about a resource in a region, you can open the resource page in Region Object Manager.<br>4. If you want to know network intrusion and interference in a region, you can open the security menu in Region Object Manager to view rogue devices, rogue STAs, attacks, and interferers in the region.<br>eSight Operations Guide Issue 08 (2018-08-28) at 1323. |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | (Optional) Configuring Security Rules<br>You can configure security rules to classify and filter rogue APs and trigger alarm sending accordingly. Therefore, network administrators can quickly locate and handle the problems to improve network security.<br>1. Enter the region object manager.<br>2. Choose Security > Rule from the navigation tree.<br>3. Set the mask length of BSSIDs.<br>After the mask length of BSSIDs is set, rogue APs with similar BSSIDs are associated to one physical device. A larger mask length makes it easier to associate rogue APs with similar BSSIDs to one physical device.<br>For example, if this parameter is set to 4, eSight converts the last two digits of BSSIDs into binary bits and compares the last four bits of the BSSIDs. If some BSSIDs have identical last four bits, eSight associates the BSSIDs to one physical device.<br>4. Create a rule.<br>Click + Create and set basic parameters and discovery filter for the rule.<br>– Channel: Match rogue devices of the Same Channel or Neighboring Channel.<br>– SSID: Set SSID for matching rogue devices. |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | – Signal Strength: Set Strength(dBm) for matching rogue devices.<br>– Detecting the number of AP: Set AP's Number for matching rogue devices.<br>– Aggressive behavior: Specify this parameter for identifying rogue APs that make attacks.<br>– Valid users association: Identify users that have connected to rogue APs.<br>5. Prioritize the rules.<br>Each rogue device can match only one rule. When multiple rules are configured, eSight checks for a rogue device starting from the rule of the highest priority.<br>Click ^ or ∨ in the Operation column to adjust the priority.<br>eSight Operations Guide Issue 08 (2018-08-28) at 1357. *See also*, *id.* at 1475-98 (discussing attack principles that may trigger an alarm).<br>The WIDS system in eSight aids in detecting network vulnerability, including by allowing various user-defined rules that aid in detecting intrusions:<br>3.2.3 WIDS Wireless Intrusion Detection System<br>The Wireless Intrusion Detection System (WIDS) manages information about rogue devices, interference resources, and attacks, and supports type-based recognition and alarm notification based on user-defined rules. Besides, the WIDS allows users to take countermeasures against unauthorized devices, ensuring wireless network security.<br>Information about rogue devices |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | |

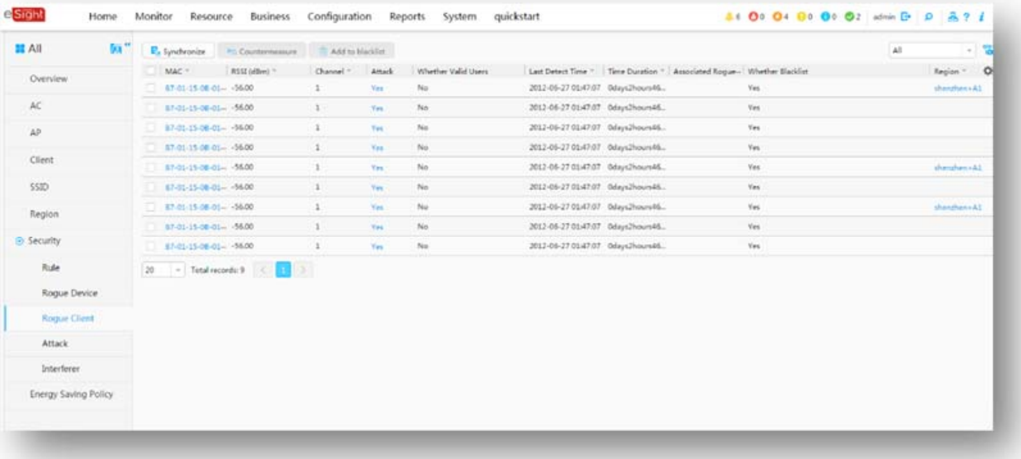


| □ | MAC | Device Type | SSID | Channel | Attack | Last Detect Time | Time Duration | Operation |
|---|---|---|---|---|---|---|---|---|
| □ | 87-01-15-08-01-09 | Rogue adHoc | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| □ | 87-01-15-08-01-21 | Rogue adHoc | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| □ | 87-01-15-08-01-15 | Rogue adHoc | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| □ | 87-01-15-08-01-45 | Rogue adHoc | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| □ | 87-01-15-08-01-39 | Rogue adHoc | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| □ | 87-01-15-08-01-36 | Rogue bridge | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| □ | 87-01-15-08-01-2A | Rogue bridge | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| □ | 87-01-15-08-01-24 | Rogue AP | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | ▤ |
| □ | 87-01-15-08-01-18 | Rogue AP | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | ▤ |
| □ | 87-01-15-08-01-3C | Rogue AP | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | ▤ |
| □ | 87-01-15-08-01-30 | Rogue AP | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | ▤ |
| □ | 87-01-15-08-01-2D | Rogue adHoc | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| □ | 87-01-15-08-01-48 | Rogue AP | wlanaccess100.0 | 1 | No | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | ▤ |
| □ | 87-01-15-08-01-1A | Rogue bridge | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| □ | 87-01-15-08-01-0E | Rogue bridge | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| □ | 87-01-15-08-01-0C | Rogue AP | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | ▤ |
| □ | 87-01-15-08-01-32 | Rogue bridge | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| □ | 87-01-15-08-02-10 | Rogue AP | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | ▤ |
| □ | 87-01-15-08-01-11 | Rogue adHoc | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| □ | 87-01-15-08-01-05 | Rogue adHoc | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |

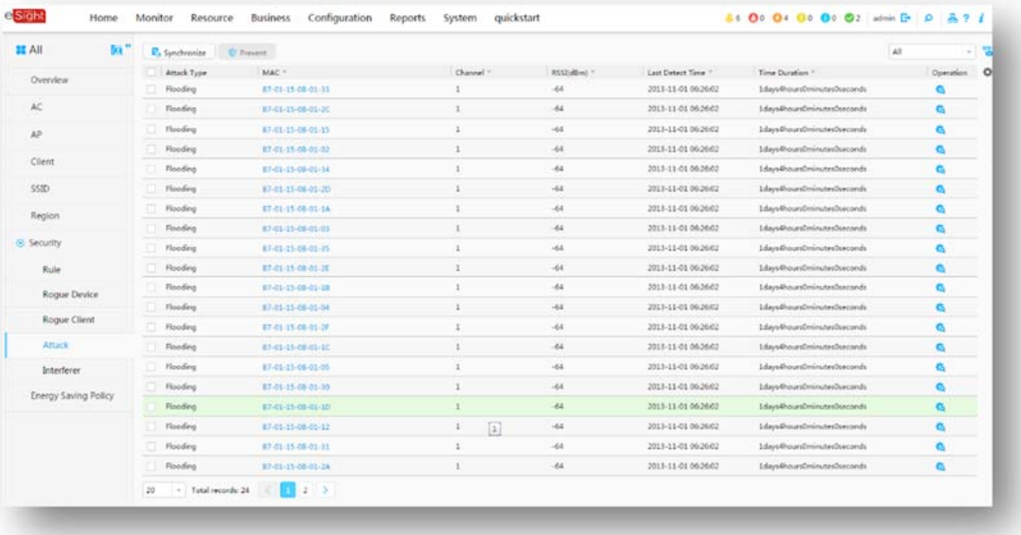
20 Total records: 52 < 1 2 3 >

Display the list, classification, and distribution of rogue devices.

Information about rogue clients

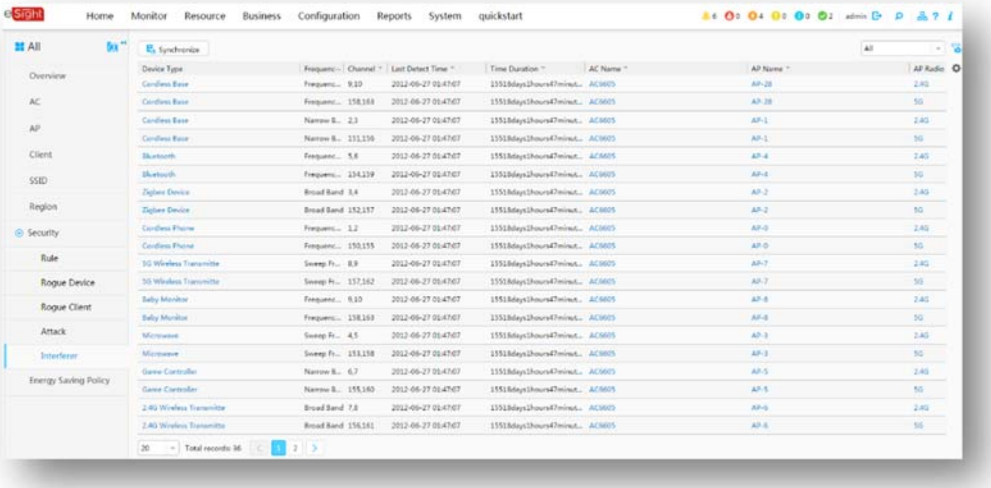
<table>
<tr><th>'227 PATENT CLAIM 1</th><th>INFRINGEMENT BY HUAWEI CORPORATION</th></tr>
<tr><td></td><td>


<table>
<tr><th>MAC</th><th>RSSI (dBm)</th><th>Channel</th><th>Attack</th><th>Whether Valid Users</th><th>Last Detect Time</th><th>Time Duration</th><th>Associated Rogue...</th><th>Whether Blacklist</th><th>Region</th></tr>
<tr><td>87-01-15-08-01-...</td><td>-56.00</td><td>1</td><td>Yes</td><td>No</td><td>2012-06-27 01:47:07</td><td>0days2hours46...</td><td></td><td>Yes</td><td>shenzhen+A1</td></tr>
<tr><td>87-01-15-08-01-...</td><td>-56.00</td><td>1</td><td>Yes</td><td>No</td><td>2012-06-27 01:47:07</td><td>0days2hours46...</td><td></td><td>Yes</td><td></td></tr>
<tr><td>87-01-15-08-01-...</td><td>-56.00</td><td>1</td><td>Yes</td><td>No</td><td>2012-06-27 01:47:07</td><td>0days2hours46...</td><td></td><td>Yes</td><td></td></tr>
<tr><td>87-01-15-08-01-...</td><td>-56.00</td><td>1</td><td>Yes</td><td>No</td><td>2012-06-27 01:47:07</td><td>0days2hours46...</td><td></td><td>Yes</td><td></td></tr>
<tr><td>87-01-15-08-01-...</td><td>-56.00</td><td>1</td><td>Yes</td><td>No</td><td>2012-06-27 01:47:07</td><td>0days2hours46...</td><td></td><td>Yes</td><td>shenzhen+A1</td></tr>
<tr><td>87-01-15-08-01-...</td><td>-56.00</td><td>1</td><td>Yes</td><td>No</td><td>2012-06-27 01:47:07</td><td>0days2hours46...</td><td></td><td>Yes</td><td></td></tr>
<tr><td>87-01-15-08-01-...</td><td>-56.00</td><td>1</td><td>Yes</td><td>No</td><td>2012-06-27 01:47:07</td><td>0days2hours46...</td><td></td><td>Yes</td><td>shenzhen+A1</td></tr>
<tr><td>87-01-15-08-01-...</td><td>-56.00</td><td>1</td><td>Yes</td><td>No</td><td>2012-06-27 01:47:07</td><td>0days2hours46...</td><td></td><td>Yes</td><td></td></tr>
<tr><td>87-01-15-08-01-...</td><td>-56.00</td><td>1</td><td>Yes</td><td>No</td><td>2012-06-27 01:47:07</td><td>0days2hours46...</td><td></td><td>Yes</td><td></td></tr>
</table>
20 Total records: 9 1<br>
Display the list, association, and distribution of rogue clients<br>
Attack information
</td></tr>
</table>

| **'227 PATENT CLAIM 1** | **INFRINGEMENT BY HUAWEI CORPORATION** |
|---|---|
| | <br>Display information about attacks upon the current wireless network.<br>Interferer information |

| ☐ | Attack Type | MAC | Channel | RSSI(dBm) | Last Detect Time | Time Duration | Operation |
|---|---|---|---|---|---|---|---|
| ☐ | Flooding | 87-01-15-08-01-33 | 1 | -64 | 2013-11-01 06:26:02 | 1days4hours0minutes0seconds | |
| ☐ | Flooding | 87-01-15-08-01-2C | 1 | -64 | 2013-11-01 06:26:02 | 1days4hours0minutes0seconds | |
| ☐ | Flooding | 87-01-15-08-01-15 | 1 | -64 | 2013-11-01 06:26:02 | 1days4hours0minutes0seconds | |
| ☐ | Flooding | 87-01-15-08-01-02 | 1 | -64 | 2013-11-01 06:26:02 | 1days4hours0minutes0seconds | |
| ☐ | Flooding | 87-01-15-08-01-34 | 1 | -64 | 2013-11-01 06:26:02 | 1days4hours0minutes0seconds | |
| ☐ | Flooding | 87-01-15-08-01-2D | 1 | -64 | 2013-11-01 06:26:02 | 1days4hours0minutes0seconds | |
| ☐ | Flooding | 87-01-15-08-01-1A | 1 | -64 | 2013-11-01 06:26:02 | 1days4hours0minutes0seconds | |
| ☐ | Flooding | 87-01-15-08-01-03 | 1 | -64 | 2013-11-01 06:26:02 | 1days4hours0minutes0seconds | |
| ☐ | Flooding | 87-01-15-08-01-35 | 1 | -64 | 2013-11-01 06:26:02 | 1days4hours0minutes0seconds | |
| ☐ | Flooding | 87-01-15-08-01-2E | 1 | -64 | 2013-11-01 06:26:02 | 1days4hours0minutes0seconds | |
| ☐ | Flooding | 87-01-15-08-01-1B | 1 | -64 | 2013-11-01 06:26:02 | 1days4hours0minutes0seconds | |
| ☐ | Flooding | 87-01-15-08-01-04 | 1 | -64 | 2013-11-01 06:26:02 | 1days4hours0minutes0seconds | |
| ☐ | Flooding | 87-01-15-08-01-2F | 1 | -64 | 2013-11-01 06:26:02 | 1days4hours0minutes0seconds | |
| ☐ | Flooding | 87-01-15-08-01-1C | 1 | -64 | 2013-11-01 06:26:02 | 1days4hours0minutes0seconds | |
| ☐ | Flooding | 87-01-15-08-01-05 | 1 | -64 | 2013-11-01 06:26:02 | 1days4hours0minutes0seconds | |
| ☐ | Flooding | 87-01-15-08-01-30 | 1 | -64 | 2013-11-01 06:26:02 | 1days4hours0minutes0seconds | |
| ☐ | Flooding | 87-01-15-08-01-1D | 1 | -64 | 2013-11-01 06:26:02 | 1days4hours0minutes0seconds | |
| ☐ | Flooding | 87-01-15-08-01-12 | 1 | -64 | 2013-11-01 06:26:02 | 1days4hours0minutes0seconds | |
| ☐ | Flooding | 87-01-15-08-01-31 | 1 | -64 | 2013-11-01 06:26:02 | 1days4hours0minutes0seconds | |
| ☐ | Flooding | 87-01-15-08-01-2A | 1 | -64 | 2013-11-01 06:26:02 | 1days4hours0minutes0seconds | |

20 Total records: 24 1 2

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |  |

| Device Type | Frequenc... | Channel | Last Detect Time | Time Duration | AC Name | AP Name | AP Radio |
|---|---|---|---|---|---|---|---|
| Cordless Base | Frequenc... | 9,10 | 2012-06-27 01:47:07 | 15518days1hours47minut... | AC6605 | AP-28 | 2.4G |
| Cordless Base | Frequenc... | 158,163 | 2012-06-27 01:47:07 | 15518days1hours47minut... | AC6605 | AP-28 | 5G |
| Cordless Base | Narrow B... | 2,3 | 2012-06-27 01:47:07 | 15518days1hours47minut... | AC6605 | AP-1 | 2.4G |
| Cordless Base | Narrow B... | 151,156 | 2012-06-27 01:47:07 | 15518days1hours47minut... | AC6605 | AP-1 | 5G |
| Bluetooth | Frequenc... | 5,8 | 2012-06-27 01:47:07 | 15518days1hours47minut... | AC6605 | AP-4 | 2.4G |
| Bluetooth | Frequenc... | 134,139 | 2012-06-27 01:47:07 | 15518days1hours47minut... | AC6605 | AP-4 | 5G |
| Zigbee Device | Broad Band | 3,4 | 2012-06-27 01:47:07 | 15518days1hours47minut... | AC6605 | AP-2 | 2.4G |
| Zigbee Device | Broad Band | 152,157 | 2012-06-27 01:47:07 | 15518days1hours47minut... | AC6605 | AP-2 | 5G |
| Cordless Phone | Frequenc... | 1,2 | 2012-06-27 01:47:07 | 15518days1hours47minut... | AC6605 | AP-0 | 2.4G |
| Cordless Phone | Frequenc... | 150,155 | 2012-06-27 01:47:07 | 15518days1hours47minut... | AC6605 | AP-0 | 5G |
| 5G Wireless Transmitte | Sweep Fr... | 8,9 | 2012-06-27 01:47:07 | 15518days1hours47minut... | AC6605 | AP-7 | 2.4G |
| 5G Wireless Transmitte | Sweep Fr... | 157,162 | 2012-06-27 01:47:07 | 15518days1hours47minut... | AC6605 | AP-7 | 5G |
| Baby Monitor | Frequenc... | 9,10 | 2012-06-27 01:47:07 | 15518days1hours47minut... | AC6605 | AP-8 | 2.4G |
| Baby Monitor | Frequenc... | 158,163 | 2012-06-27 01:47:07 | 15518days1hours47minut... | AC6605 | AP-8 | 5G |
| Microwave | Sweep Fr... | 4,5 | 2012-06-27 01:47:07 | 15518days1hours47minut... | AC6605 | AP-3 | 2.4G |
| Microwave | Sweep Fr... | 153,158 | 2012-06-27 01:47:07 | 15518days1hours47minut... | AC6605 | AP-3 | 5G |
| Game Controller | Narrow B... | 6,7 | 2012-06-27 01:47:07 | 15518days1hours47minut... | AC6605 | AP-5 | 2.4G |
| Game Controller | Narrow B... | 155,160 | 2012-06-27 01:47:07 | 15518days1hours47minut... | AC6605 | AP-5 | 5G |
| 2.4G Wireless Transmitte | Broad Band | 7,8 | 2012-06-27 01:47:07 | 15518days1hours47minut... | AC6605 | AP-6 | 2.4G |
| 2.4G Wireless Transmitte | Broad Band | 156,161 | 2012-06-27 01:47:07 | 15518days1hours47minut... | AC6605 | AP-6 | 5G |

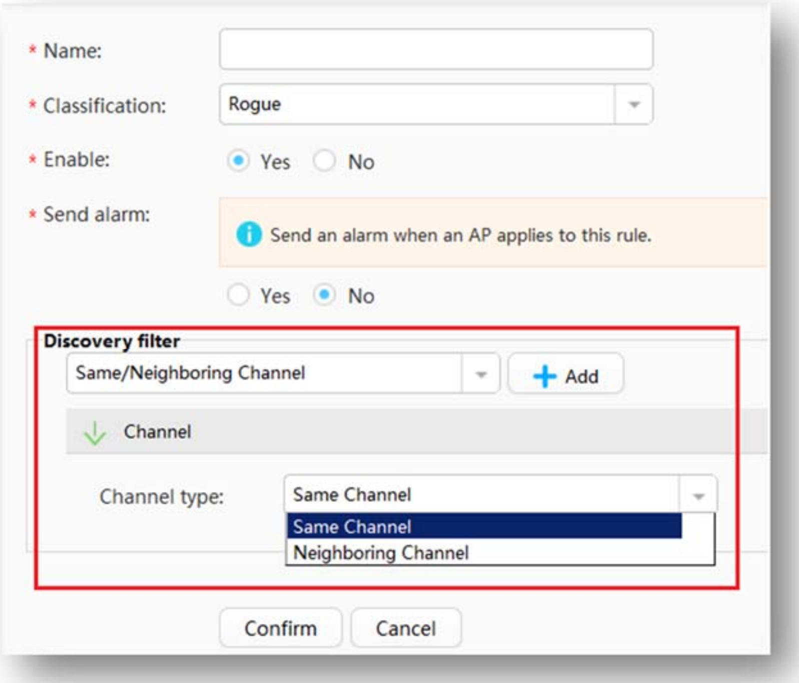
20 Total records: 36 1 2

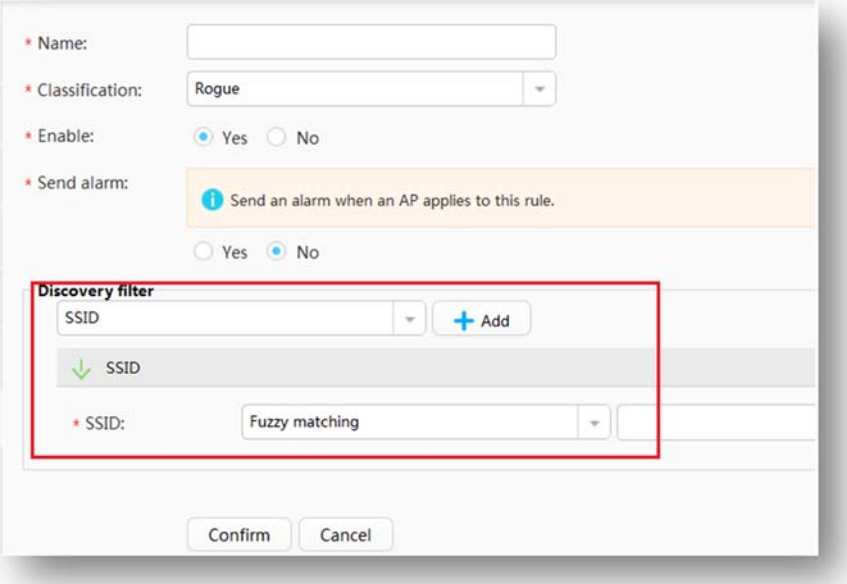
Display the interferer list, interference on APs, and interference relationships in the location topology by subnet.

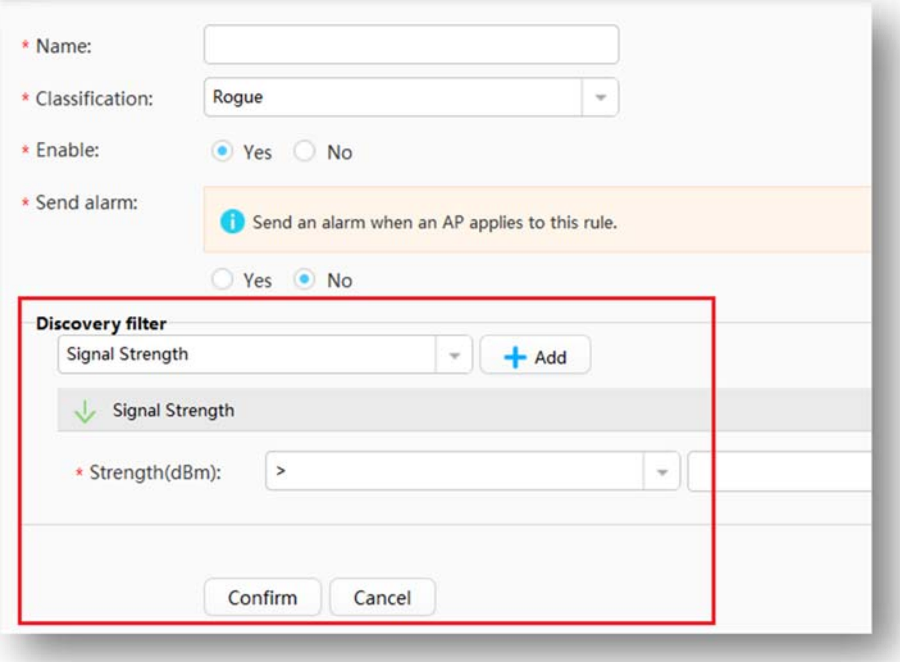
Rule definition

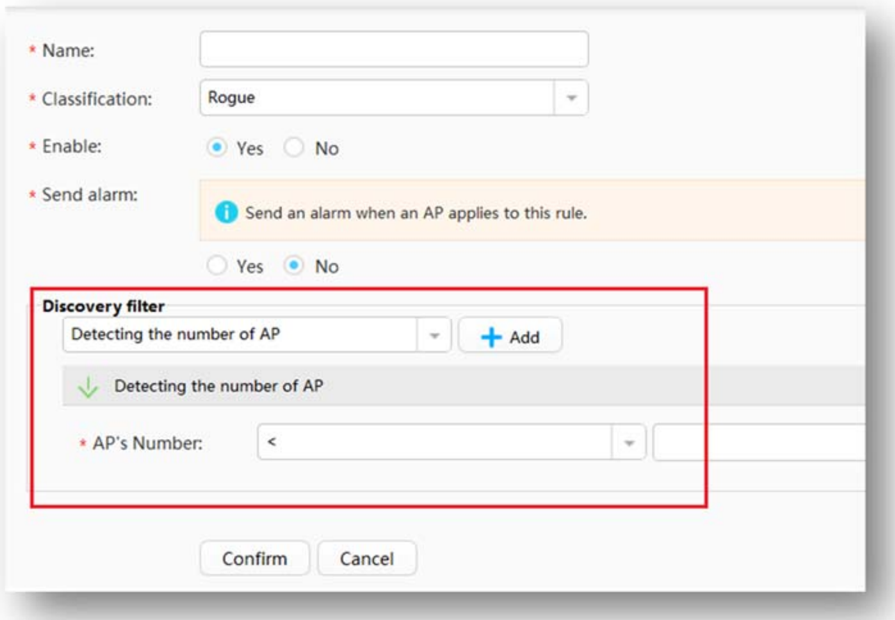
Network administrators can classify and filter rogue APs and management alarms based on defined rules. Rule definition involves the following indicators: SSID, channel, field strength, impact scope, and attack behavior. Users can enable eSight to generate alarms when rogue APs in compliance with defined rules are detected.

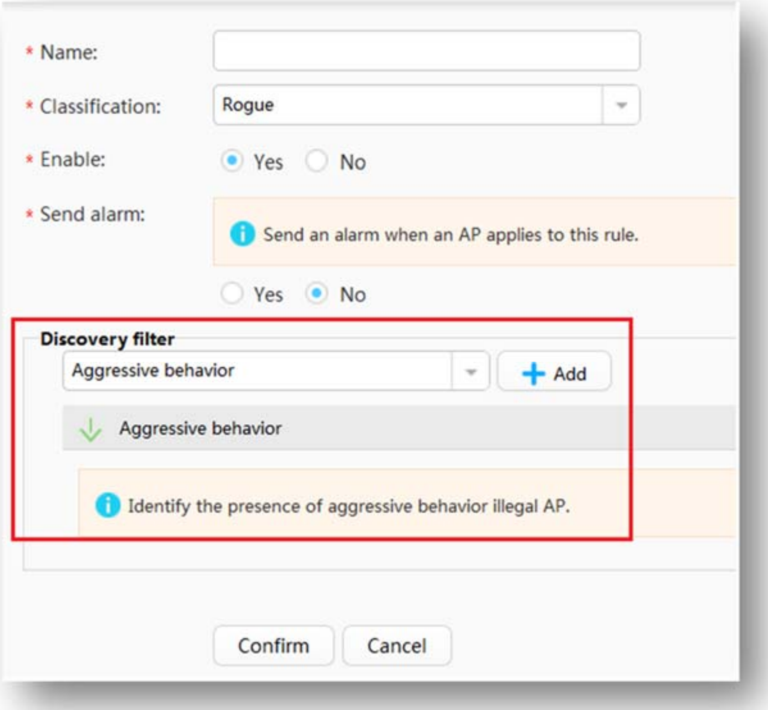
Same or adjacent channel

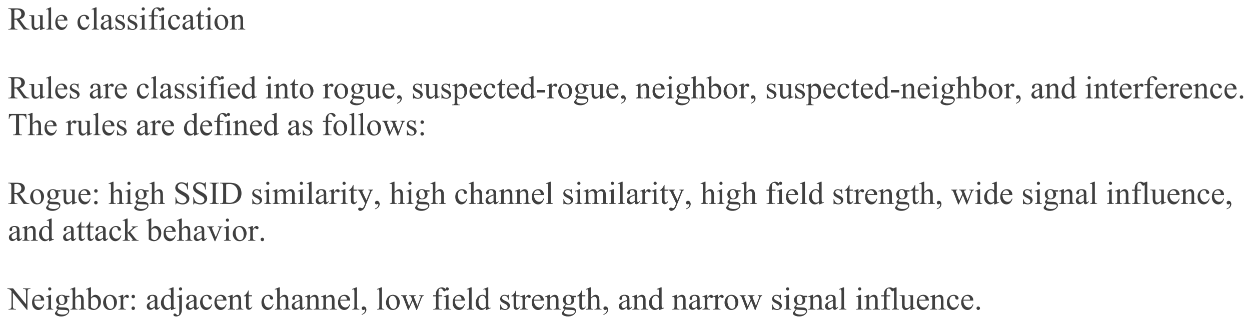
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | This rule is used to detect the channel deployment of APs, and detect rogue APs that operate in the same or adjacent channel. If rogue APs operate in the same channel with normal APs, eSight regards it as same-frequency interference; if rogue APs operate in an adjacent channel, eSight regards it as adjacent-frequency interference<br><br>* Name:<br>* Classification: Rogue<br>* Enable: ● Yes ○ No<br>* Send alarm: Send an alarm when an AP applies to this rule. ○ Yes ● No<br>Discovery filter<br>Same/Neighboring Channel<br>Channel<br>Channel type: Same Channel<br> + Add<br>Same Channel<br>Neighboring Channel<br>Confirm<br>Cancel |

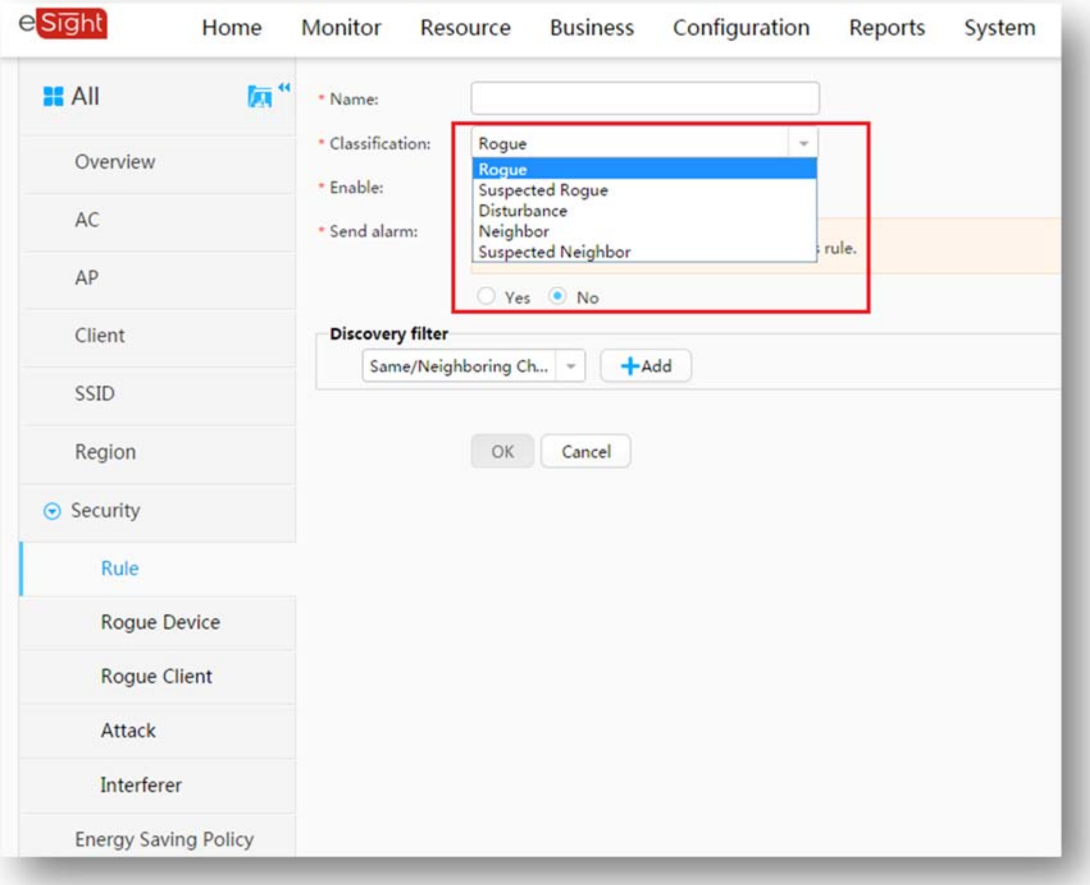
| ’227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | SSID<br>The service set identifiers of networks from unauthorized vendors or wireless networks established by individuals are similar to authorized SSIDs. For example, the SSIDs are the same or characters are similar (such as 0 and o). In this case, users may be deceived to log in to rogue wireless networks. An SSID rule can be used to detect rogue APs whose SSIDs are similar to the authorized SSIDs or when a specified rule (regular expression) is met.<br><br>* Name:<br>* Classification: Rogue<br>* Enable: ● Yes ○ No<br>* Send alarm: Send an alarm when an AP applies to this rule.<br>○ Yes ● No<br>Discovery filter<br>SSID + Add<br>SSID<br>* SSID: Fuzzy matching<br>Confirm Cancel |

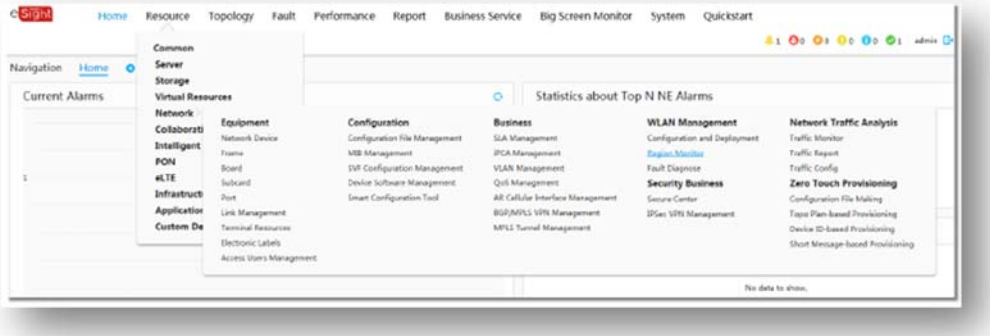
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | Signal strength<br>Users can set field strength thresholds to recognize high-field-strength wireless signals that may interfere authorized APs. If the signal strength exceeds the specified thresholds, eSight regards it as high-field-strength interference.<br><br>* Name:<br>* Classification: Rogue<br>* Enable: ● Yes ○ No<br>* Send alarm: Send an alarm when an AP applies to this rule.<br>○ Yes ● No<br>Discovery filter<br>Signal Strength<br>Signal Strength<br>* Strength(dBm): ><br> |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | Number of detecting APs<br>Users can specify the threshold for the number of detecting APs rule to recognize wireless signals that may interfere a large number of authorized APs. If the number of APs that detect a rogue AP exceeds the threshold, eSight regards it as large-scale interference.<br><br>* Name:<br>* Classification: Rogue<br>* Enable: ● Yes ○ No<br>* Send alarm: Send an alarm when an AP applies to this rule.<br>○ Yes ● No<br>Discovery filter<br>Detecting the number of AP<br>Detecting the number of AP<br>* AP's Number: <<br> |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | Attack behavior<br>This rule is used to detect attacks from rogue APs on wireless networks. Users can define attack behavior rules to recognize rogue APs that attacked authorized APs.<br><br>* Name:<br>* Classification: Rogue<br>* Enable: ● Yes ○ No<br>* Send alarm: Send an alarm when an AP applies to this rule.<br>○ Yes ● No<br>Discovery filter<br>Aggressive behavior<br>Aggressive behavior<br>Identify the presence of aggressive behavior illegal AP.<br> |

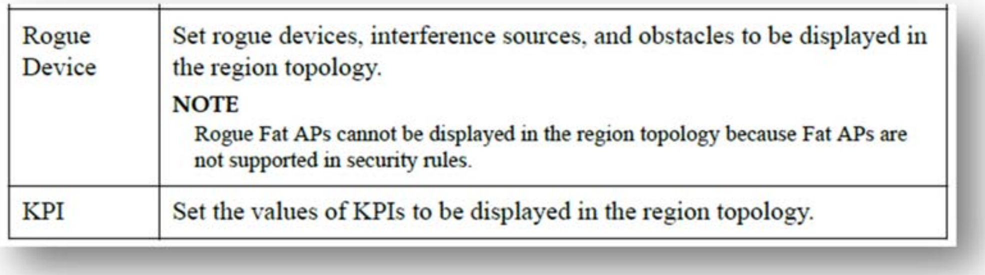
| **'227 PATENT CLAIM 1** | **INFRINGEMENT BY HUAWEI CORPORATION** |
|---|---|
| | <br>Rule classification<br>Rules are classified into rogue, suspected-rogue, neighbor, suspected-neighbor, and interference. The rules are defined as follows:<br>Rogue: high SSID similarity, high channel similarity, high field strength, wide signal influence, and attack behavior.<br>Neighbor: adjacent channel, low field strength, and narrow signal influence. |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | <br> eSight<br>Home<br>Monitor<br>Resource<br>Business<br>Configuration<br>Reports<br>System<br>All<br>Overview<br>AC<br>AP<br>Client<br>SSID<br>Region<br>Security<br>Rule<br>Rogue Device<br>Rogue Client<br>Attack<br>Interferer<br>Energy Saving Policy<br>Rogue<br>Suspected Rogue<br>Disturbance<br>Neighbor<br>Suspected Neighbor<br>rule.<br>+Add<br>OK<br>Cancel<br>* Name:<br>* Classification: Rogue<br>* Enable:<br>* Send alarm: ○ Yes ● No<br>Discovery filter: Same/Neighboring Ch...<br>HUAWEI eSight WLAN White Paper Issue 01 (2017-03-20) at 10-16 |

| **'227 PATENT CLAIM 1** | **INFRINGEMENT BY HUAWEI CORPORATION** |
|---|---|
| | Rogue devices can also be viewed in the region topology along with KPI indicators, for example:<br>12.11.5 Network Monitoring<br>eSight allows network administrators to view information about a WLAN, including service performance counters, user access records, network security threats. According to such information, network administrators can determine the overall WLAN conditions.<br>…<br>Configuring Items to Be Displayed in the Region Topology<br>1. Choose Resource > Network > WLAN Management > Region Monitor from the main menu.<br><br> eSight<br>Home<br>Resource<br>Topology<br>Fault<br>Performance<br>Report<br>Business Service<br>Big Screen Monitor<br>System<br>Quickstart<br>admin<br>Navigation<br>Home<br>Current Alarms<br>Statistics about Top N NE Alarms<br>Common<br>Server<br>Storage<br>Virtual Resources<br>Network<br>Collaborati<br>Intelligent<br>PON<br>eLTE<br>Infrastruct<br>Applicatio<br>Custom De<br>Equipment<br>Network Device<br>Frame<br>Board<br>Subcard<br>Port<br>Link Management<br>Terminal Resources<br>Electronic Labels<br>Access Users Management<br>Configuration<br>Configuration File Management<br>MIB Management<br>SVF Configuration Management<br>Device Software Management<br>Smart Configuration Tool<br>Business<br>SLA Management<br>IPCA Management<br>VLAN Management<br>QoS Management<br>AR Cellular Interface Management<br>BGP/MPLS VPN Management<br>MPLS Tunnel Management<br>WLAN Management<br>Configuration and Deployment<br>Region Monitor<br>Fault Diagnose<br>Security Business<br>Secure Center<br>IPSec VPN Management<br>Network Traffic Analysis<br>Traffic Monitor<br>Traffic Report<br>Traffic Config<br>Zero Touch Provisioning<br>Configuration File Making<br>Topo Plan-based Provisioning<br>Device ID-based Provisioning<br>Short Message-based Provisioning<br>No data to show.<br>2. Select a bottom-layer region, click Monitor, and click in the topology toolbar in the monitoring mode. |

<table>
<tr><th>'227 PATENT CLAIM 1</th><th>INFRINGEMENT BY HUAWEI CORPORATION</th></tr>
<tr><td></td><td>

…

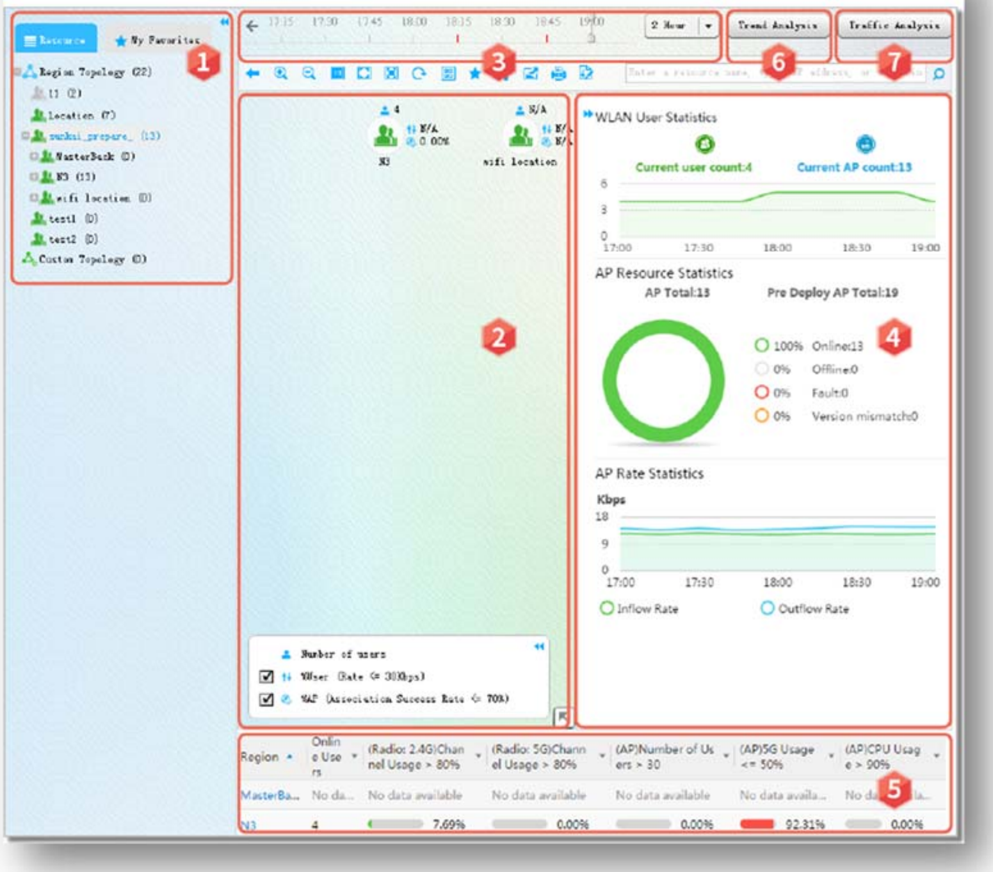


<table>
<tr><td>Rogue Device</td><td>Set rogue devices, interference sources, and obstacles to be displayed in the region topology.<br>NOTE<br>Rogue Fat APs cannot be displayed in the region topology because Fat APs are not supported in security rules.</td></tr>
<tr><td>KPI</td><td>Set the values of KPIs to be displayed in the region topology.</td></tr>
</table>

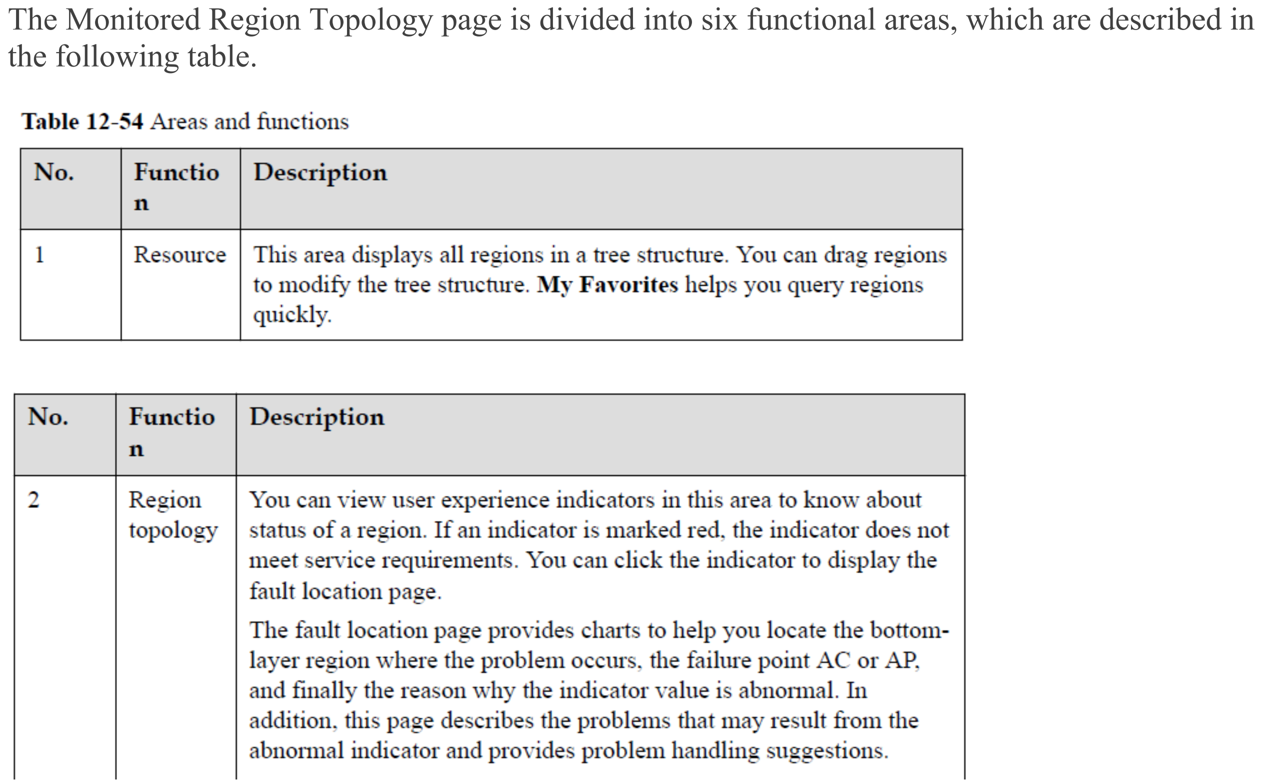
eSight Operations Guide Issue 08 (2018-08-28) at 1353.

On information and belief, when a vulnerable device causes an alarm to trigger, it results in the network map changing a different color indicative of the vulnerability, for example, the object is displayed in the region topology in red:

</td></tr>
</table>

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | **Figure 12-25** Region topology view<br><br> Resource<br>My Favorites<br>1<br>Region Topology (22)<br>11 (2)<br>Location (7)<br>sunkai_prepare_ (13)<br>MasterBack (0)<br>N3 (13)<br>wifi location (0)<br>test1 (0)<br>test2 (0)<br>Custom Topology (0)<br>17:15 17:30 17:45 18:00 18:15 18:30 18:45 19:00<br>2 Hour<br>Trend Analysis<br>Traffic Analysis<br>3<br>6<br>7<br>4<br>N/A<br>0.00%<br>N3<br>wifi location<br>2<br>WLAN User Statistics<br>Current user count:4<br>Current AP count:13<br>6<br>3<br>0<br>17:00 17:30 18:00 18:30 19:00<br>AP Resource Statistics<br>AP Total:13<br>Pre Deploy AP Total:19<br>4<br>100% Online:13<br>0% Offline:0<br>0% Fault:0<br>0% Version mismatch:0<br>AP Rate Statistics<br>Kbps<br>18<br>9<br>0<br>17:00 17:30 18:00 18:30 19:00<br>Inflow Rate<br>Outflow Rate<br>Number of users<br>☑ %User (Rate <= 30Kbps)<br>☑ %AP (Association Success Rate <= 70%)<br>5<br>Region ▲ \| Online Users \| (Radio: 2.4G)Channel Usage > 80% \| (Radio: 5G)Channel Usage > 80% \| (AP)Number of Users > 30 \| (AP)5G Usage <= 50% \| (AP)CPU Usage > 90%<br>MasterBa... \| No da... \| No data available \| No data available \| No data available \| No data availa... \| No da... la...<br>N3 \| 4 \| 7.69% \| 0.00% \| 0.00% \| 92.31% \| 0.00% |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | |



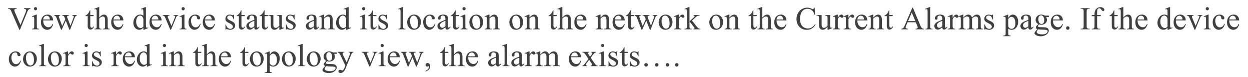
The Monitored Region Topology page is divided into six functional areas, which are described in the following table.

**Table 12-54** Areas and functions

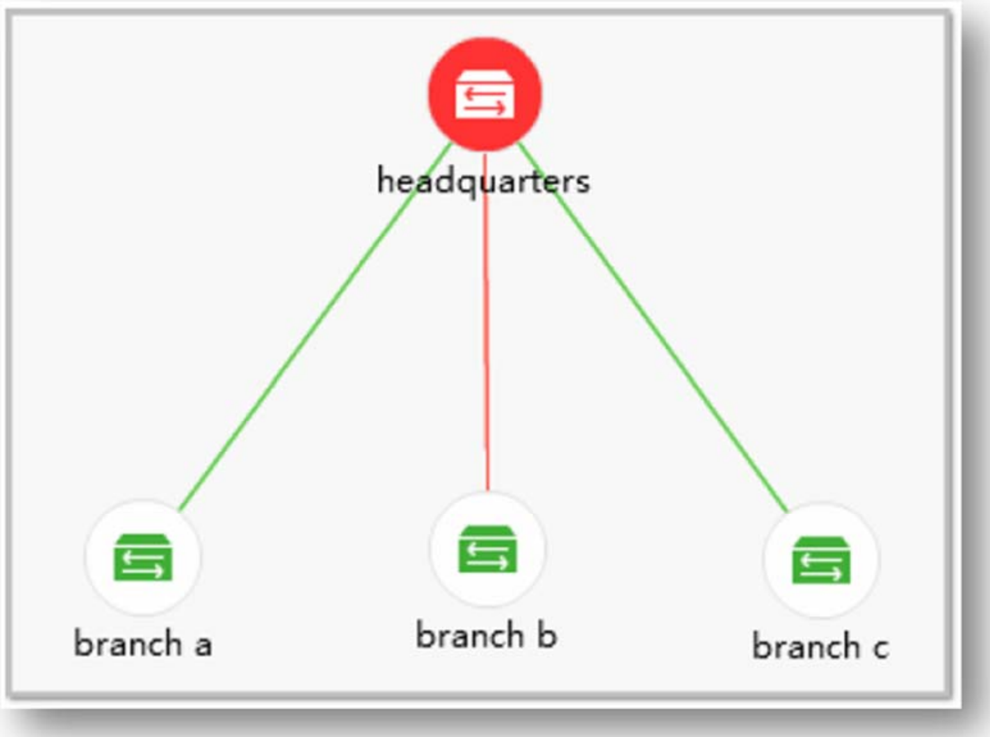
| No. | Function | Description |
|---|---|---|
| 1 | Resource | This area displays all regions in a tree structure. You can drag regions to modify the tree structure. **My Favorites** helps you query regions quickly. |

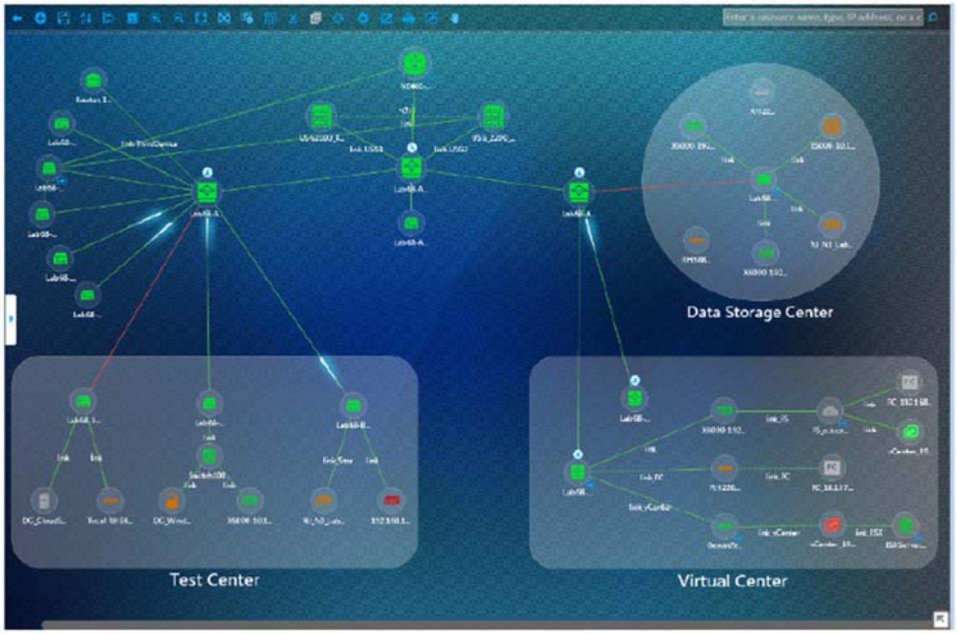
| No. | Function | Description |
|---|---|---|
| 2 | Region topology | You can view user experience indicators in this area to know about status of a region. If an indicator is marked red, the indicator does not meet service requirements. You can click the indicator to display the fault location page.<br>The fault location page provides charts to help you locate the bottom-layer region where the problem occurs, the failure point AC or AP, and finally the reason why the indicator value is abnormal. In addition, this page describes the problems that may result from the abnormal indicator and provides problem handling suggestions. |

eSight Operations Guide Issue 08 (2018-08-28) at 1358-59.



View the device status and its location on the network on the Current Alarms page. If the device color is red in the topology view, the alarm exists….

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |  <br>eSight Operations Guide Issue 08 (2018-08-28) at 235.<br>The eSight provides various alarm monitoring methods and multidimensional alarm data statistics. |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
|  | …<br>- Monitor alarms on a topology<br>**Figure 5-3** Topology<br><br> <br>eSight Operations Guide Issue 08 (2018-08-28) at 213. |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | 7.3.2 Monitoring the Network Running Status in Topologies<br>eSight displays the network running status in different colors in physical and IP topologies. This is the most frequently-used network monitoring approach for a majority of users.<br>…<br>In eSight, the color, running status, and judgment standard and rectification method for abnormal status vary according to the topology object type.<br>Table 7-3 provides the mapping between running status and icon colors for subnets and devices. |

| '227 Patent Claim 1 | Infringement By Huawei Corporation |
|---|---|
| | |

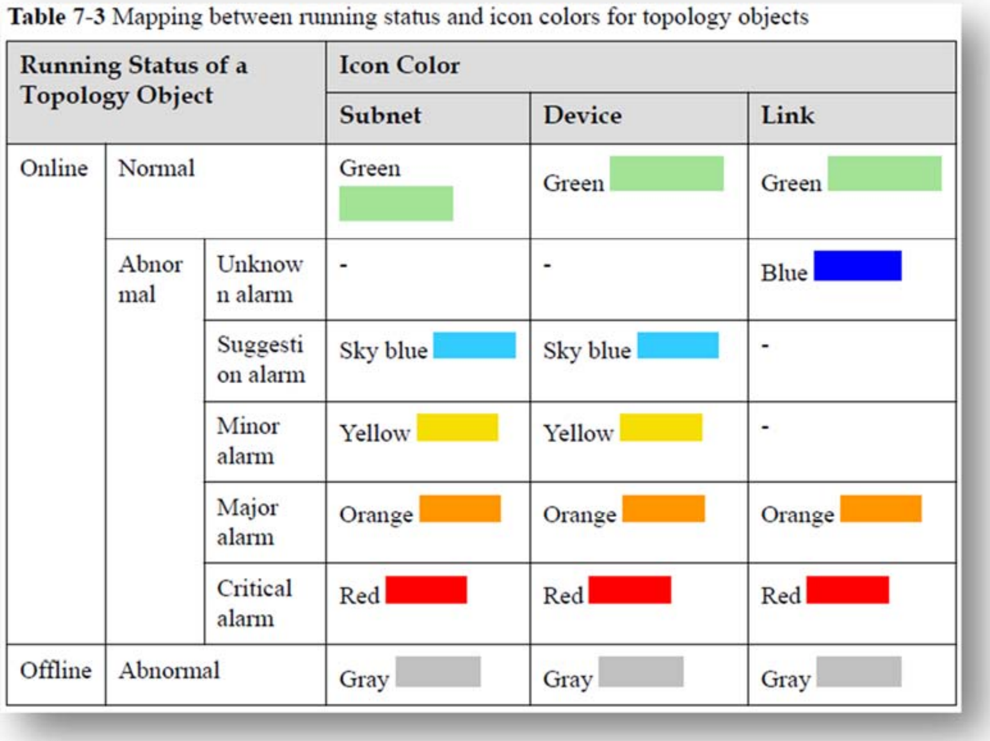
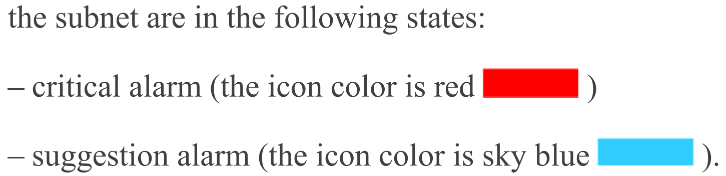
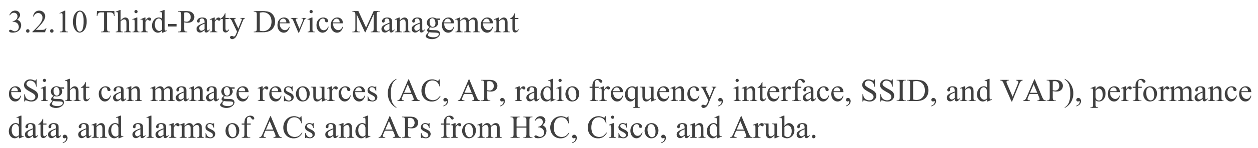
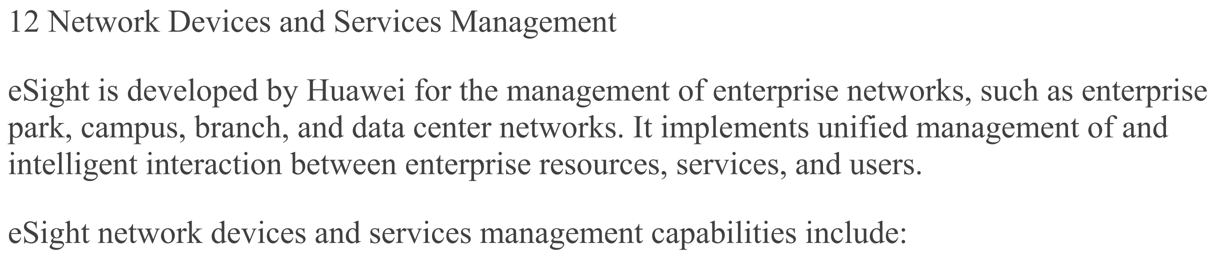


Table 7-3 Mapping between running status and icon colors for topology objects

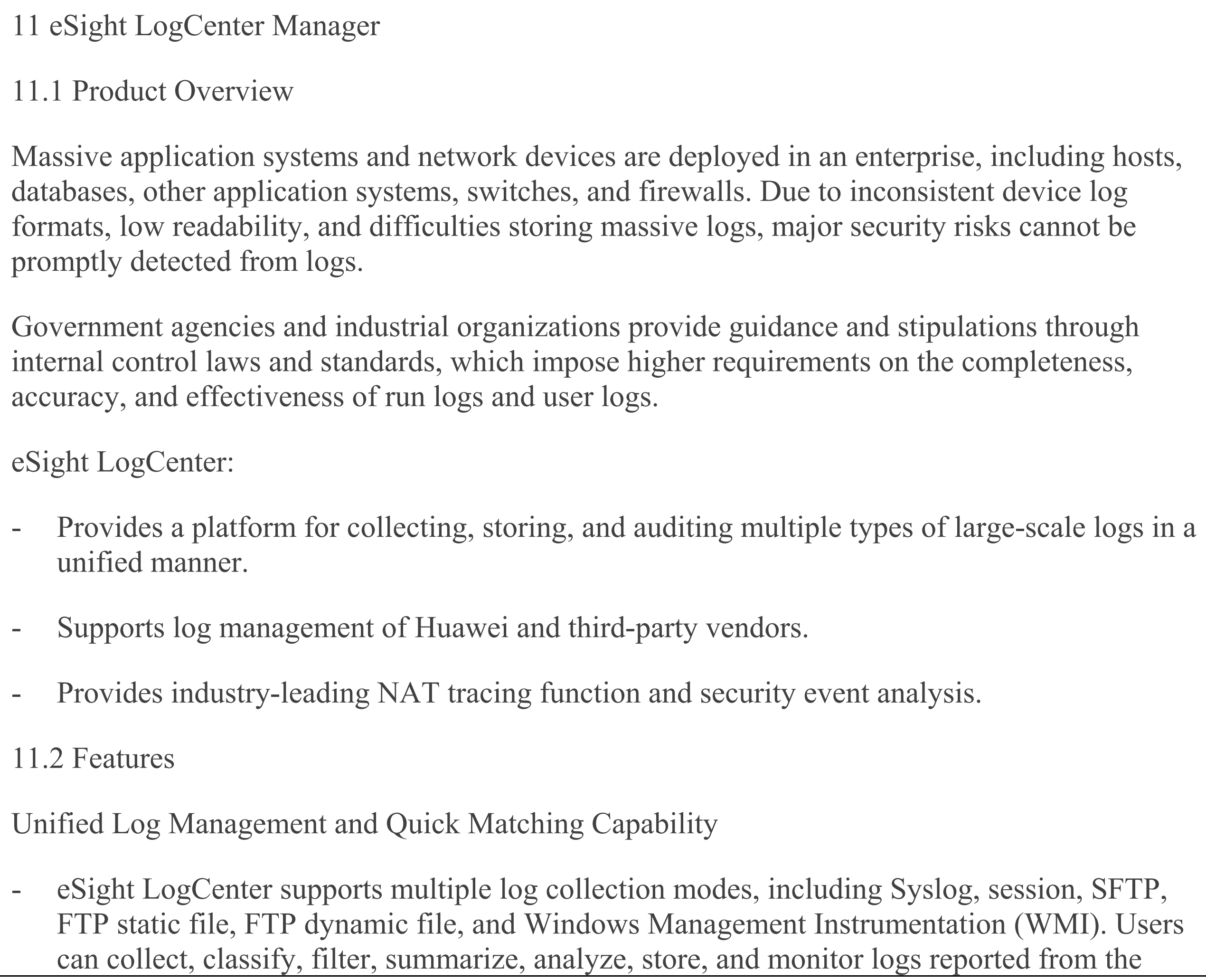
| Running Status of a Topology Object | | | Icon Color | | |
|---|---|---|---|---|---|
| | | | Subnet | Device | Link |
| Online | Normal | | Green 🟩 | Green 🟩 | Green 🟩 |
| | Abnormal | Unknown alarm | - | - | Blue 🟦 |
| | | Suggestion alarm | Sky blue 🟦 | Sky blue 🟦 | - |
| | | Minor alarm | Yellow 🟨 | Yellow 🟨 | - |
| | | Major alarm | Orange 🟧 | Orange 🟧 | Orange 🟧 |
| | | Critical alarm | Red 🟥 | Red 🟥 | Red 🟥 |
| Offline | Abnormal | | Gray ⬜ | Gray ⬜ | Gray ⬜ |

…

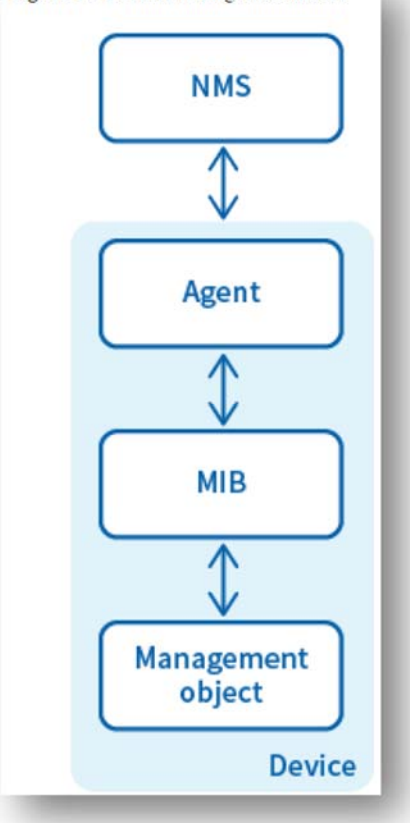
A subnet is in the critical alarm state (the icon color is red 🔴 ) when devices on

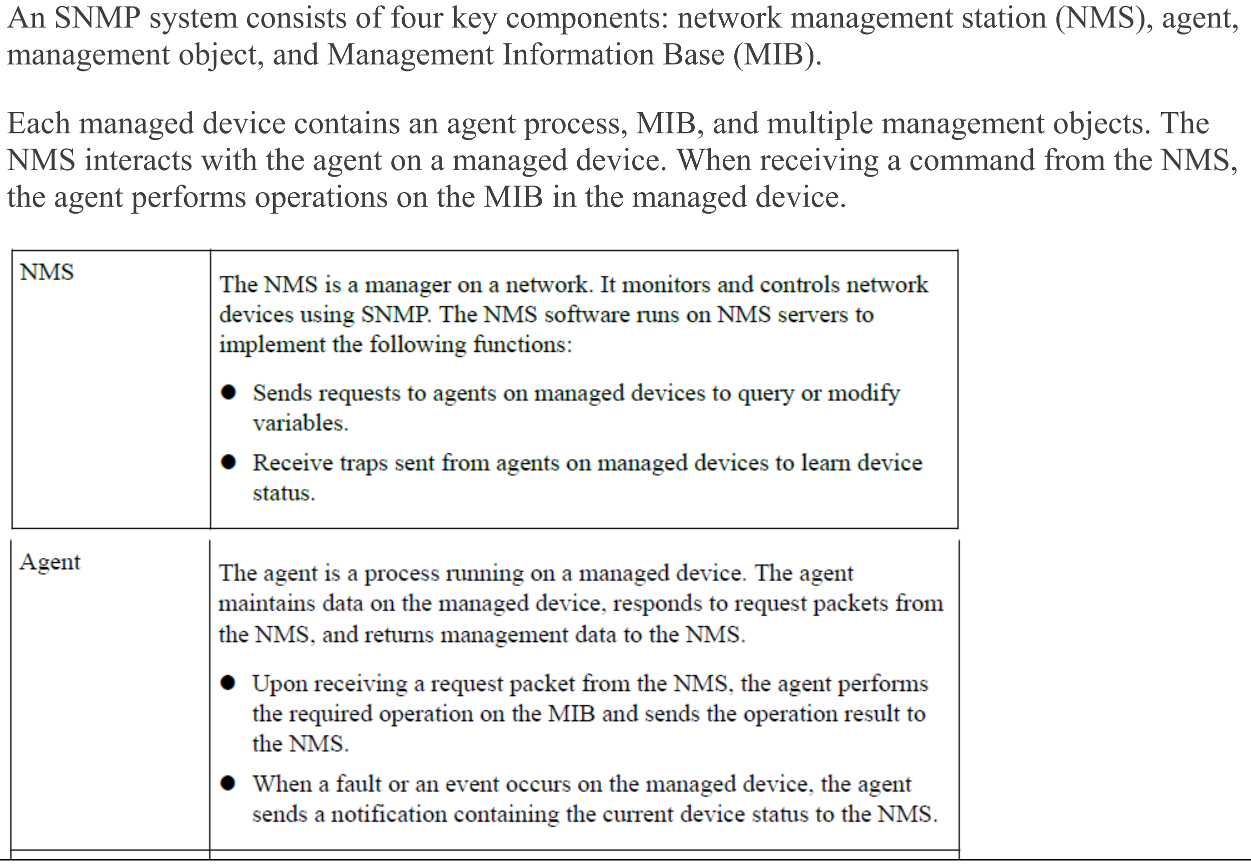
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |  the subnet are in the following states:<br>– critical alarm (the icon color is red 🟥 )<br>– suggestion alarm (the icon color is sky blue 🟦 ).<br>eSight Operations Guide Issue 08 (2018-08-28) at 303-04<br>eSight is capable of detecting vulnerable nodes and manages the alarms, performance, configurations, and security of devices from multiple vendors on a network. Further, on information and belief, each device may have its own management system:<br> 3.2.10 Third-Party Device Management<br>eSight can manage resources (AC, AP, radio frequency, interface, SSID, and VAP), performance data, and alarms of ACs and APs from H3C, Cisco, and Aruba.<br>HUAWEI eSight WLAN White Paper Issue 01 (2017-03-20) at 22.<br> 12 Network Devices and Services Management<br>eSight is developed by Huawei for the management of enterprise networks, such as enterprise park, campus, branch, and data center networks. It implements unified management of and intelligent interaction between enterprise resources, services, and users.<br>eSight network devices and services management capabilities include: |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | - Manages the alarms, performance, configurations, and security of devices from multiple vendors on a network in a unified manner.<br>- Monitors and manages wireless local area networks (WLANs).<br>- Monitors and manages Multiprotocol Label Switching (MPLS) virtual private networks (VPNs).<br>- Monitors and analyzes network quality through service level agreement (SLA) Manager and Network Traffic Analyzer (NTA).<br>eSight Operations Guide Issue 08 (2018-08-28) at 1023.<br>For example, the eSight management platform Product Datasheet explains:<br>Enterprises are using an increasing number of core and access devices provided by multiple vendors. Each device has its own management system, creating confusion for system and network administrators.<br>To alleviate the operational burden, Huawei has developed the eSight Management Platform, a unified network management system that provides a comprehensive view and management of all network and system resources, ensures network stability, and improves O&M efficiency.<br>The eSight Management Platform provides compact, standard, and professional editions for enterprise users. It supports unified management of devices from various vendors, topology management, fault management, performance management, and user right management.<br>Huawei eSight Full Product Datasheet Issue (2013-09-03) at 5.<br>Further, the eSight LogCenter Manager aids in detecting security risks from both Huawei and third-party vendors. |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | <br>11 eSight LogCenter Manager<br>11.1 Product Overview<br>Massive application systems and network devices are deployed in an enterprise, including hosts, databases, other application systems, switches, and firewalls. Due to inconsistent device log formats, low readability, and difficulties storing massive logs, major security risks cannot be promptly detected from logs.<br>Government agencies and industrial organizations provide guidance and stipulations through internal control laws and standards, which impose higher requirements on the completeness, accuracy, and effectiveness of run logs and user logs.<br>eSight LogCenter:<br>- Provides a platform for collecting, storing, and auditing multiple types of large-scale logs in a unified manner.<br>- Supports log management of Huawei and third-party vendors.<br>- Provides industry-leading NAT tracing function and security event analysis.<br>11.2 Features<br>Unified Log Management and Quick Matching Capability<br>- eSight LogCenter supports multiple log collection modes, including Syslog, session, SFTP, FTP static file, FTP dynamic file, and Windows Management Instrumentation (WMI). Users can collect, classify, filter, summarize, analyze, store, and monitor logs reported from the |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | application systems or NEs to help the administrator manage massive logs and learn NE running status, trace network user behavior, and quickly recognize and eliminate security risks.<br>Huawei eSight Full Product Datasheet Issue (2013-09-03) at 43.<br>On information and belief, the eSight LogCenter manager, in connection with the Management Information Base, allows a security posture of the network to be established by correlating a system object model database that supports information data requirements of disparate network vulnerability analysis programs with any data results obtained from the programs. For example:<br>If eSight is connected to the LogCenter, the LogCenter must be added using the ICMP protocol and only SNMPv2c alarms can be received.<br>Huawei eSight Full Product Datasheet Issue (2013-09-03) at 214.<br>Comprehensive Device Management Capabilities<br>eSight can manage devices from multiple manufacturers, including network devices from Huawei, H3C, Cisco, and ZTE, and IT devices from IBM, HP, and Sun. It also allows you to customize device types for management. Customized device types can be managed in the same way as preconfigured device types.<br>• eSight manages non-Huawei devices that support standard management information base (MIB) (RFC1213-MIB, Entity-MIB, SNMPv2-MIB, and IF-MIB) through user-defined settings.<br>• eSight manages non-Huawei devices that do not support MIB through network element (NE) adaptation packages.<br>http://support.huawei.com/hedex/pages/EDOC1000014129DYC0111A/04/EDOC1000014129DYC0111A/04/resources/pd/en-us_topic_0002514480.html?ft=99&id=EN-US_TOPIC_0002514480&keyword=mib&text=Features&docid=EDOC1000014129 |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | **Figure 12-1** SNMP management model<br><br> |

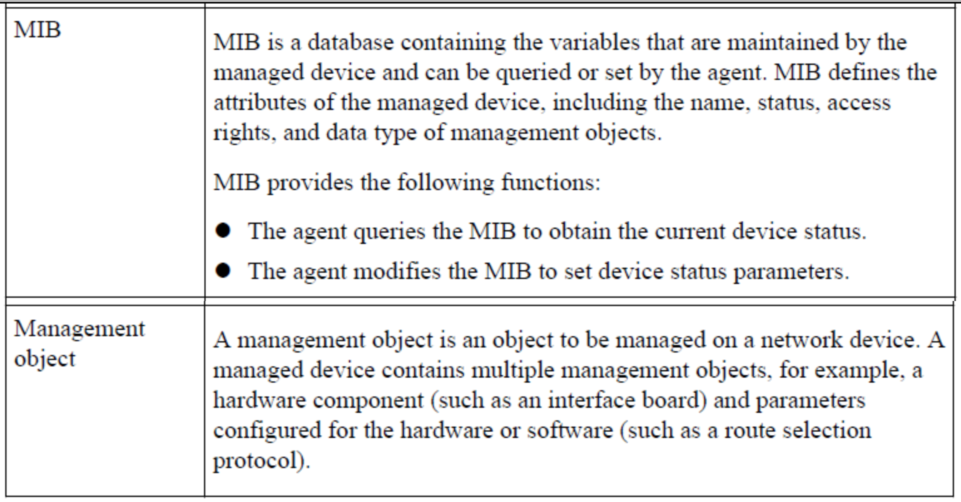
<table>
<tr><th>'227 PATENT CLAIM 1</th><th>INFRINGEMENT BY HUAWEI CORPORATION</th></tr>
<tr><td></td><td>


An SNMP system consists of four key components: network management station (NMS), agent, management object, and Management Information Base (MIB).

Each managed device contains an agent process, MIB, and multiple management objects. The NMS interacts with the agent on a managed device. When receiving a command from the NMS, the agent performs operations on the MIB in the managed device.

<table>
<tr><td>NMS</td><td>The NMS is a manager on a network. It monitors and controls network devices using SNMP. The NMS software runs on NMS servers to implement the following functions:<br>● Sends requests to agents on managed devices to query or modify variables.<br>● Receive traps sent from agents on managed devices to learn device status.</td></tr>
<tr><td>Agent</td><td>The agent is a process running on a managed device. The agent maintains data on the managed device, responds to request packets from the NMS, and returns management data to the NMS.<br>● Upon receiving a request packet from the NMS, the agent performs the required operation on the MIB and sends the operation result to the NMS.<br>● When a fault or an event occurs on the managed device, the agent sends a notification containing the current device status to the NMS.</td></tr>
</table>
</td></tr>
</table>

| '227 Patent Claim 1 | Infringement By Huawei Corporation |
|---|---|

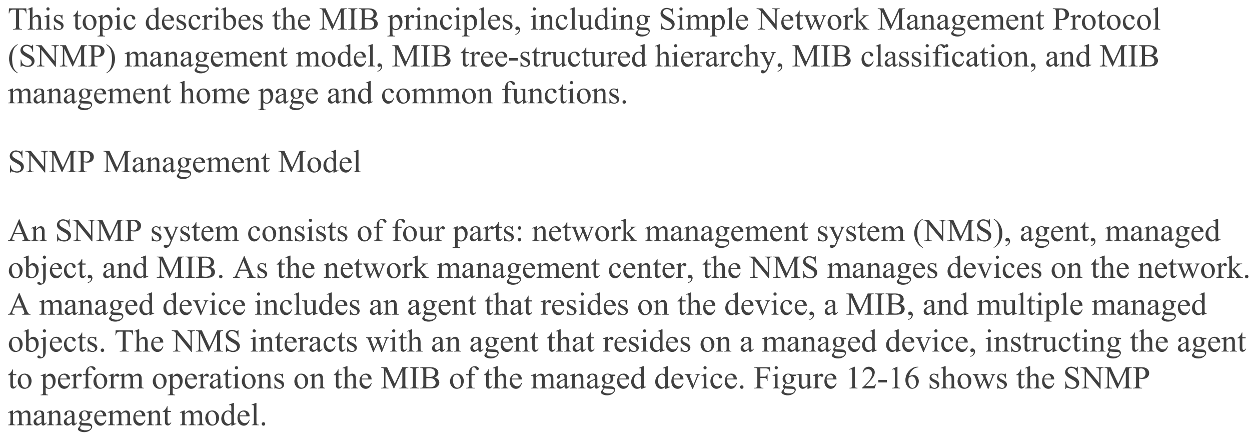


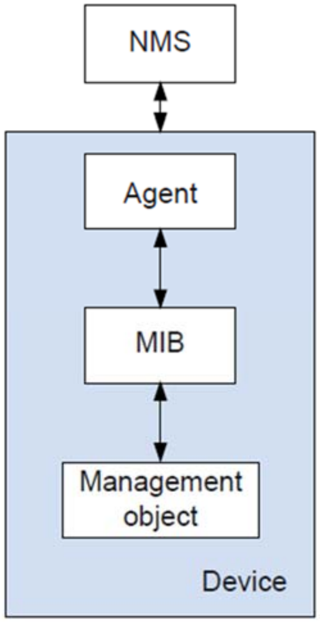
| | |
|---|---|
| MIB | MIB is a database containing the variables that are maintained by the managed device and can be queried or set by the agent. MIB defines the attributes of the managed device, including the name, status, access rights, and data type of management objects.<br>MIB provides the following functions:<br>● The agent queries the MIB to obtain the current device status.<br>● The agent modifies the MIB to set device status parameters. |
| Management object | A management object is an object to be managed on a network device. A managed device contains multiple management objects, for example, a hardware component (such as an interface board) and parameters configured for the hardware or software (such as a route selection protocol). |

eSight Operations Guide Issue 08 (2018-08-28) at 1024-25

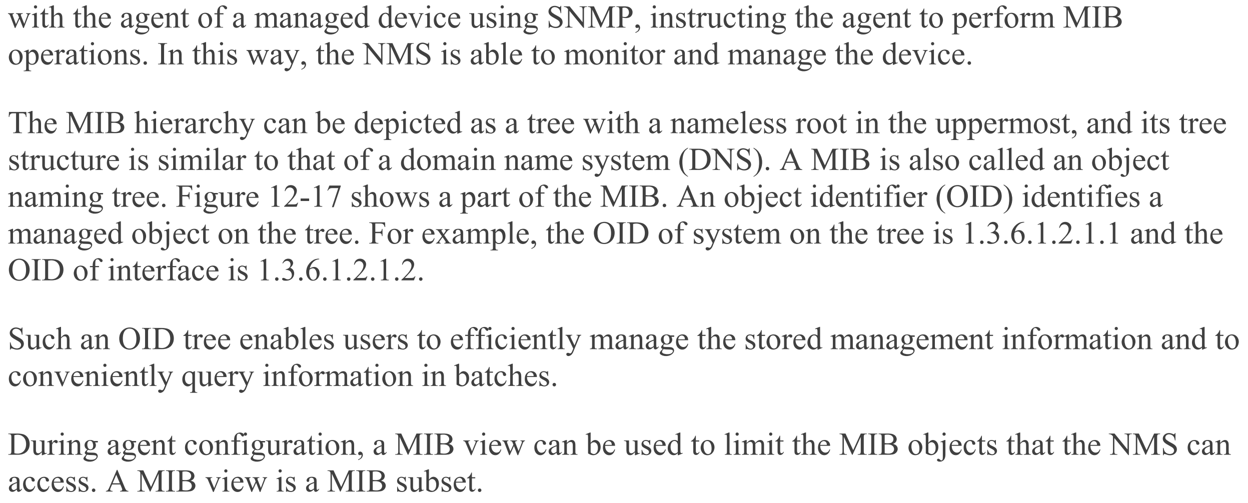
The MIB management tool contains a system object model database, for example:

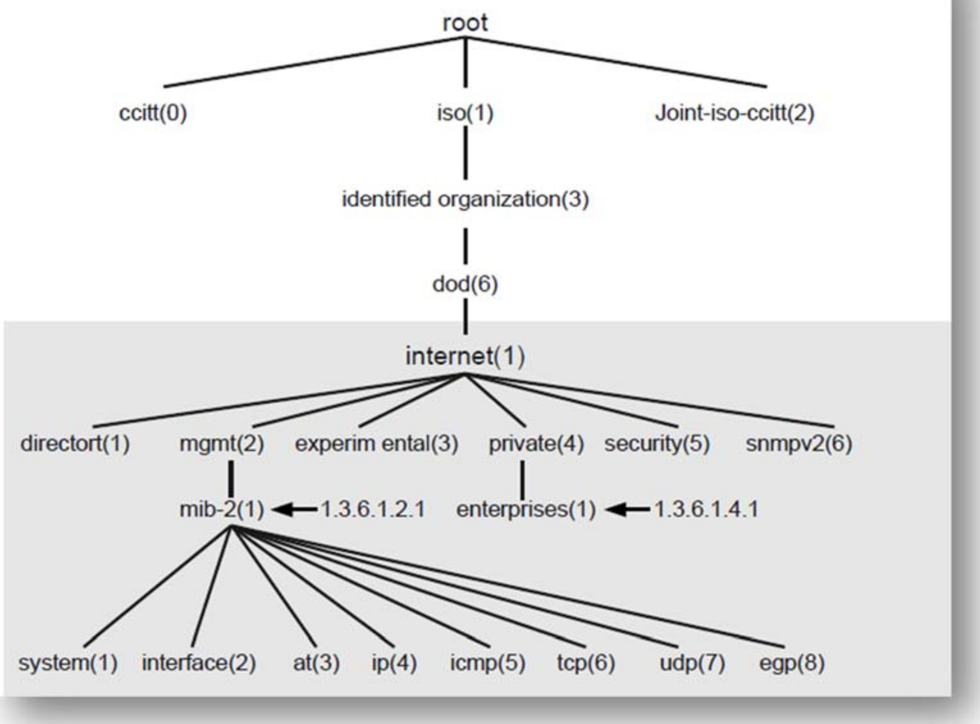
> 12.5 MIB Management
>
> Management Information Base (MIB) Management is a tool designed for managing MIBs. This tool displays MIB objects in a tree-structured hierarchy and supports common MIB operations, including Get, GetNext, Walk, TableView, Stop, MIB file compiling, and MIB file loading.
>
> 12.5.1 Function Overview

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | <br>This topic describes the MIB principles, including Simple Network Management Protocol (SNMP) management model, MIB tree-structured hierarchy, MIB classification, and MIB management home page and common functions.<br>SNMP Management Model<br>An SNMP system consists of four parts: network management system (NMS), agent, managed object, and MIB. As the network management center, the NMS manages devices on the network. A managed device includes an agent that resides on the device, a MIB, and multiple managed objects. The NMS interacts with an agent that resides on a managed device, instructing the agent to perform operations on the MIB of the managed device. Figure 12-16 shows the SNMP management model. |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | **Figure 12-16** SNMP management model<br><br> <br>The following describes the four parts in an SNMP system:<br>- NMS<br>The NMS runs on the NMS server to manage and monitor network devices using SNMP. |

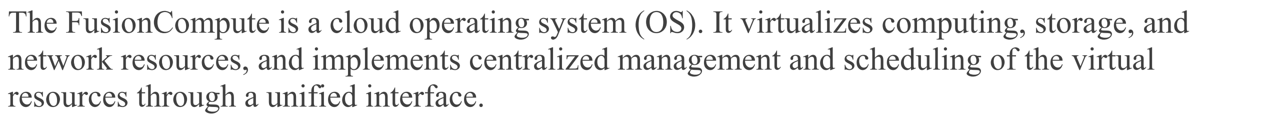
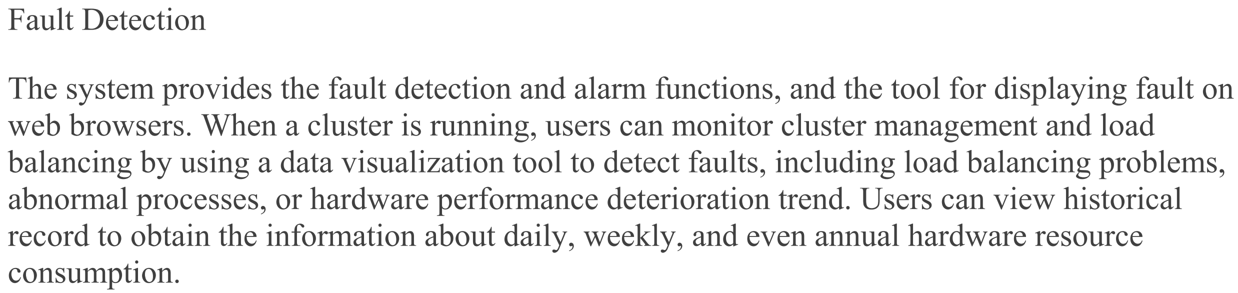
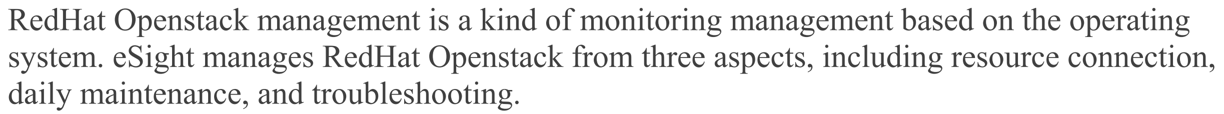
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | – The NMS sends requests to the agent of a managed device for querying or modifying one or more parameters.<br>– The NMS receives trap information actively sent from the agent of a managed device to obtain the status of the managed device.<br>- Agent<br>An agent is a process that runs on a managed device for maintaining data of the managed device, responding to the requests sent from the NMS, and sending management data to the NMS.<br>– An agent receives requests from the NMS, performs related operations on the MIB tables, and sends the operation results to the NMS.<br>– When a device encounters a fault event or any other exceptions, the device actively reports its status change to the NMS through the agent.<br>- Managed object<br>A managed object is an object that is managed by the NMS. It can be a piece of hardware (for example, an interface board) on a device or a collection of hardware or software (for example, a routing selection protocol) and associated configuration parameters. A device may have multiple managed objects.<br>- MIB<br>A MIB is a database that specifies variables (information that can be queried and set by an agent) maintained by a managed device. It defines a series of attributes for a managed device, including the object name, object status, object access rights, and object data type. The NMS communicates |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | <br>with the agent of a managed device using SNMP, instructing the agent to perform MIB operations. In this way, the NMS is able to monitor and manage the device.<br>The MIB hierarchy can be depicted as a tree with a nameless root in the uppermost, and its tree structure is similar to that of a domain name system (DNS). A MIB is also called an object naming tree. Figure 12-17 shows a part of the MIB. An object identifier (OID) identifies a managed object on the tree. For example, the OID of system on the tree is 1.3.6.1.2.1.1 and the OID of interface is 1.3.6.1.2.1.2.<br>Such an OID tree enables users to efficiently manage the stored management information and to conveniently query information in batches.<br>During agent configuration, a MIB view can be used to limit the MIB objects that the NMS can access. A MIB view is a MIB subset. |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | **Figure 12-17** OID tree structure<br><br> root<br>ccitt(0)<br>iso(1)<br>Joint-iso-ccitt(2)<br>identified organization(3)<br>dod(6)<br>internet(1)<br>directort(1)<br>mgmt(2)<br>experim ental(3)<br>private(4)<br>security(5)<br>snmpv2(6)<br>mib-2(1)<br>1.3.6.1.2.1<br>enterprises(1)<br>1.3.6.1.4.1<br>system(1)<br>interface(2)<br>at(3)<br>ip(4)<br>icmp(5)<br>tcp(6)<br>udp(7)<br>egp(8)<br>MIB Classification<br>MIBs can be classified into two types: public MIB and proprietary MIB. |

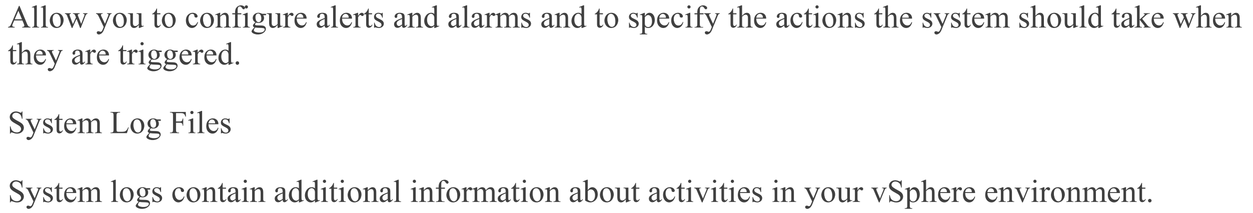
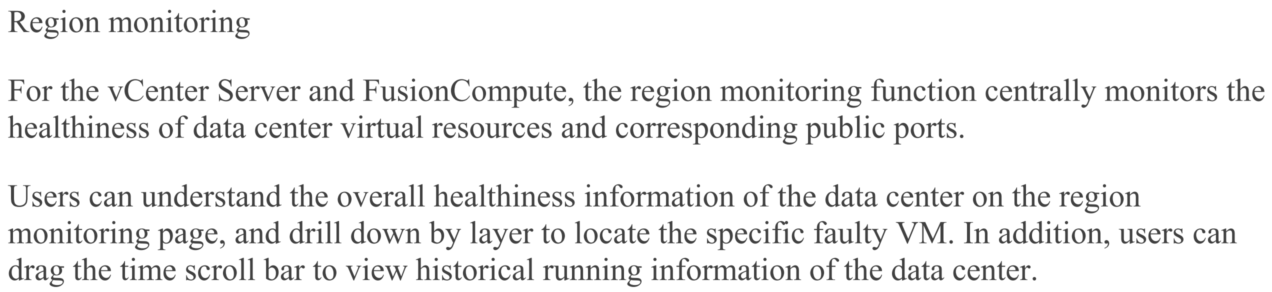
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
|  | - Public MIB: generally defined by the Requirement For Comments (RFC) for structured design and interface standardization processing for various public protocols. For example, OSPF-MIB (RFC1850) and BGP4-MIB (RFC1657) are typical public MIBs. Most of the equipment vendors provide RFC-compliant SNMP interfaces.<br>- Proprietary MIB: a necessary supplement to public MIBs. When equipment vendors develop their own proprietary protocols or unique functions, proprietary MIBs can be used to improve the management functions of SNMP interfaces. In addition, proprietary MIBs enable third-party NMS software to manage devices that use proprietary protocols or have unique functions.<br>eSight Operations Guide Issue 08 (2018-08-28) at 1162-64.<br>Further, the eSight Virtual Resource Manager network map turns a different color indicative of a vulnerability that has been established for that portion of the network after a security posture of the network has been established by correlating a system object model database that supports information data requirements of disparate network vulnerability analysis programs with any data results obtained from the programs.<br>For example, the eSight Virtual Resource Manager integrates with disparate network vulnerability analysis programs such as FusionSphere, Redhat OpenStack, FusionCompute, VMware ESX/ESXi Server, VMware vCenter Server, and, on information and belief, also utilizes a system object model database to correlate the data:<br>11 Virtual Resources Management<br>The Virtual Resource Manager can manage FusionSphere, Redhat OpenStack, FusionCompute, vCenter Servers, and ESX Servers, allowing users to obtain information about the alarms and performance of virtual resources in the system.<br>11.1 Virtual Resources Management Introduction |

| ’227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | The Virtual Resource Management feature provides basic virtual resource management functions and integrates entries for information query, maintenance, and operation of a single NE into one page, which facilitates monitoring and maintenance of a single NE.<br>11.1.1 Definition<br>The Virtual Resource Management feature provides the function of centrally monitoring virtual computing infrastructure such as the FusionSphere OpenStack, Redhat OpenStack, VMware ESX/ESXi Server, VMware vCenter Server, and FusionCompute.<br>11.1.2 Function<br>eSight provides virtual resource management functions and integrates entries for information query, maintenance, and operation of a single NE into one page, which facilitates monitoring and maintenance of a single NE.<br>Virtual Resource Access<br>The Virtual Resource Access function accesses and monitors virtual computing infrastructure such as the FusionSphere OpenStack, Redhat OpenStack, VMware ESX/ESXi Server, VMware vCenter Server, and FusionCompute.<br>eSight Operations Guide Issue 08 (2018-08-28) at 941.<br>For example, FusionCompute provides eSight with vulnerability analysis: |

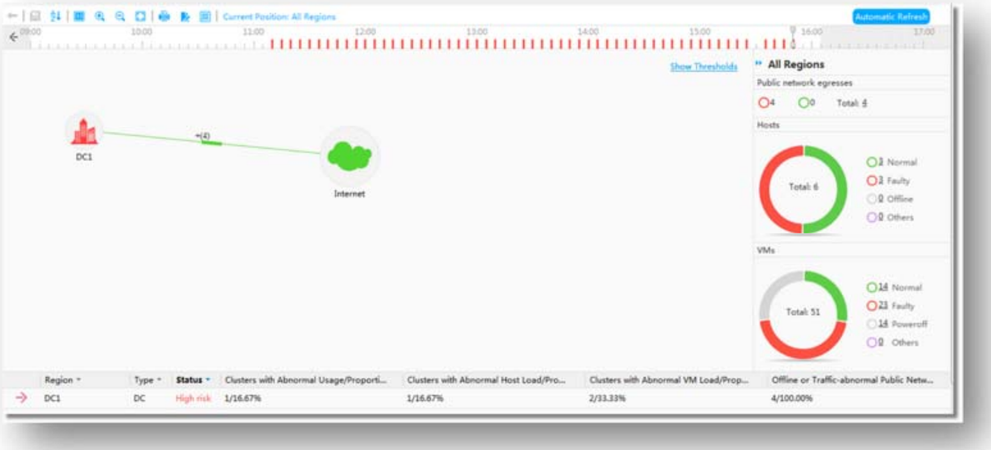
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | <br>The FusionCompute is a cloud operating system (OS). It virtualizes computing, storage, and network resources, and implements centralized management and scheduling of the virtual resources through a unified interface.<br>The FusionCompute provides high system security and reliability and reduces operational costs. It helps carriers and enterprises build secure, green, and energy-saving data centers.<br>FusionCompute Product Description Issue 01 (2015-11-11) at 2.<br><br>Fault Detection<br>The system provides the fault detection and alarm functions, and the tool for displaying fault on web browsers. When a cluster is running, users can monitor cluster management and load balancing by using a data visualization tool to detect faults, including load balancing problems, abnormal processes, or hardware performance deterioration trend. Users can view historical record to obtain the information about daily, weekly, and even annual hardware resource consumption.<br>FusionCompute Product Description Issue 01 (2015-11-11) at 42.<br>RedHat OpenStack further provides risk and vulnerability analysis, for example:<br><br>RedHat Openstack management is a kind of monitoring management based on the operating system. eSight manages RedHat Openstack from three aspects, including resource connection, daily maintenance, and troubleshooting.<br>eSight Operations Guide Issue 08 (2018-08-28) at 951. |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | 1.2. Security Boundaries and Threats<br>To understand the security risks that present themselves to your cloud deployment, it can be helpful to abstractly think about it as a collection of components that have a common function, users, and shared security concerns, which this guide refers to as security zones. Threat actors and vectors are classified based on their motivation and access to resources. The intention is to provide you a sense of the security concerns for each zone, depending on your objectives.<br>…<br>1.4. Threat classification, actors, and attack vectors<br>Most types of cloud deployment, public, private, or hybrid, are exposed to some form of attack. This section categorizes attackers and summarizes potential types of attacks in each security zone.<br>1.4.1. Threat actors<br>A threat actor is an abstract way to refer to a class of adversary that you might attempt to defend against. The more capable the actor, the more rigorous the security controls that are required for successful attack mitigation and prevention. Security is a matter of balancing convenience, defense, and cost, based on requirements. In some cases it will not be possible to secure a cloud deployment against all of the threat actors described here. When deploying an OpenStack cloud, you must decide where the balance lies for your deployment and usage.<br>…<br>In addition, Red Hat maintains a dedicated security team that analyzes threats and vulnerabilities against our products, and provides relevant advice and updates through the Customer Portal. This team determines which issues are important, as opposed to those that are mostly theoretical |

| '227 Patent Claim 1 | Infringement By Huawei Corporation |
|---|---|
| | problems. The Red Hat Product Security team maintains expertise in, and makes extensive contributions to the upstream communities associated with our subscription products. A key part of the process, Red Hat Security Advisories, deliver proactive notification of security flaws affecting Red Hat solutions – along with patches that are frequently distributed on the same day the vulnerability is first published.<br>RedHat OpenStack Platform Security and Hardening Guide, available at https://access.redhat.com/documentation/en-us/red_hat_openstack_platform/13/html-single/security_and_hardening_guide/<br>VMware vCenter Server and VMware ESX also provide risk and vulnerability analysis:<br>VMware provides several tools to help you monitor your virtual environment and to locate the source of potential issues and current problems.<br>Performance charts<br>Allow you to see performance data on a variety of system resources including CPU, Memory, Storage, and so on.<br>Performance monitoring command-line utilities<br>Allow you to access detailed information on system performance through the command line.<br>Host health<br>Allows you to quickly identify which hosts are healthy and which are experiencing problems.<br>Events, alerts, and alarms |

| '227 Patent Claim 1 | Infringement By Huawei Corporation |
|---|---|
| | <br>Allow you to configure alerts and alarms and to specify the actions the system should take when they are triggered.<br>System Log Files<br>System logs contain additional information about activities in your vSphere environment.<br>About vSphere Monitoring and Performance at 6 (available at https://docs.vmware.com/en/VMware-vSphere/6.7/vsphere-esxi-vcenter-server-671-monitoring-performance-guide.pdf)<br>The eSight Virtual Resource Manager provides region monitoring, VM component topology and VM physical topology in which network icons change color indicative of vulnerabilities:<br><br>Region monitoring<br>For the vCenter Server and FusionCompute, the region monitoring function centrally monitors the healthiness of data center virtual resources and corresponding public ports.<br>Users can understand the overall healthiness information of the data center on the region monitoring page, and drill down by layer to locate the specific faulty VM. In addition, users can drag the time scroll bar to view historical running information of the data center. |

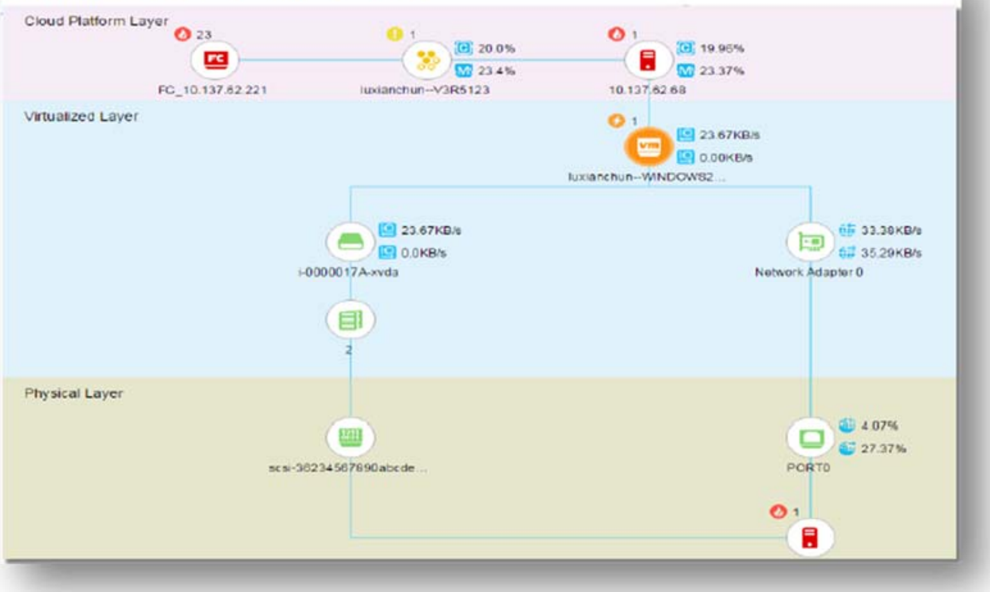
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | |



| Region | Type | Status | Clusters with Abnormal Usage/Proporti... | Clusters with Abnormal Host Load/Pro... | Clusters with Abnormal VM Load/Prop... | Offline or Traffic-abnormal Public Netw... |
|---|---|---|---|---|---|---|
| DC1 | DC | High risk | 1/16.67% | 1/16.67% | 2/33.33% | 4/100.00% |

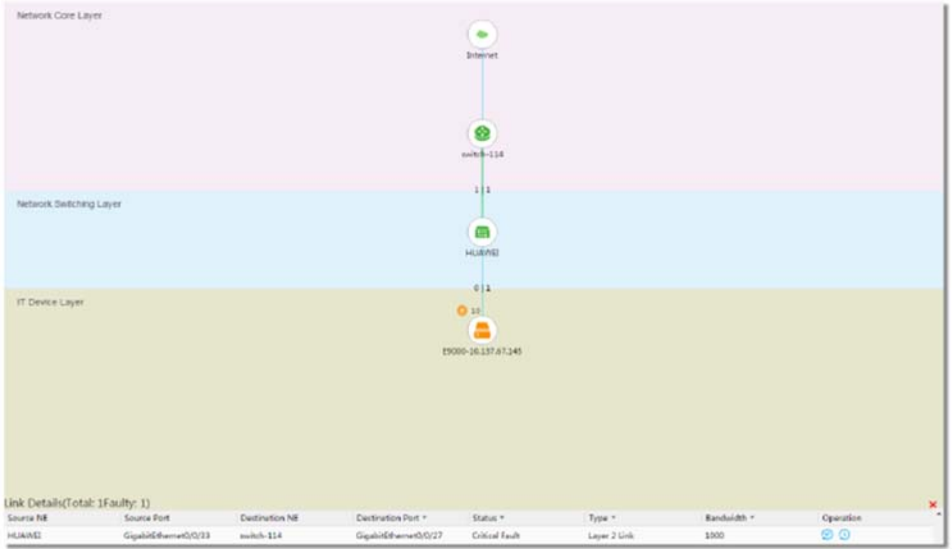
VM component topology

For the FusionSphere OpenStack and FusionCompute, O&M personnel can view virtual components such as cloud disks and ports of VMs, and view the mapping between virtual components and physical resources in the component topology.

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | **Figure 11-4** VM component topology<br><br> Cloud Platform Layer<br>23<br>FC_10.137.62.221<br>1<br>20.0%<br>23.4%<br>luxianchun--V3R5123<br>1<br>19.96%<br>23.37%<br>10.137.62.68<br>Virtualized Layer<br>1<br>23.67KB/s<br>0.00KB/s<br>luxianchun--WINDOWS2...<br>23.67KB/s<br>0.0KB/s<br>i-0000017A-xvda<br>33.38KB/s<br>35.29KB/s<br>Network Adapter 0<br>2<br>Physical Layer<br>scsi-36234567890abcde...<br>4.07%<br>27.37%<br>PORT0<br>1<br>VM physical topology<br>For the FusionSphere OpenStack and FusionCompute, O&M personnel can view the network topology from the physical device where the VM is located to the external routers from the VM perspective. |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|

**Figure 11-5** VM physical topology

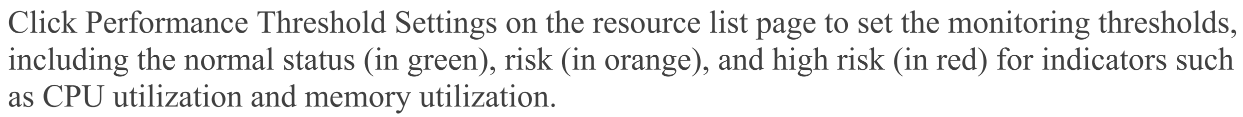
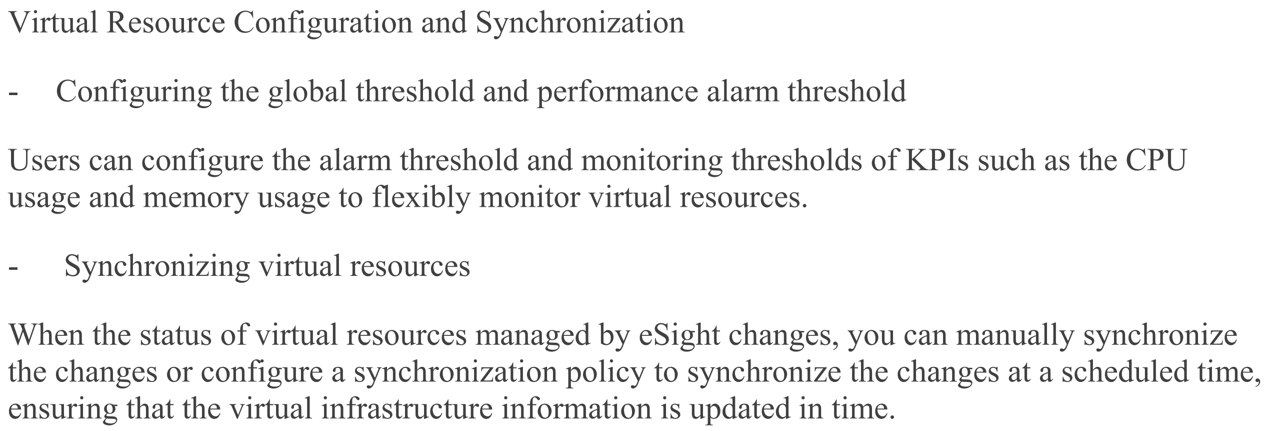


Link Details(Total: 1Faulty: 1)

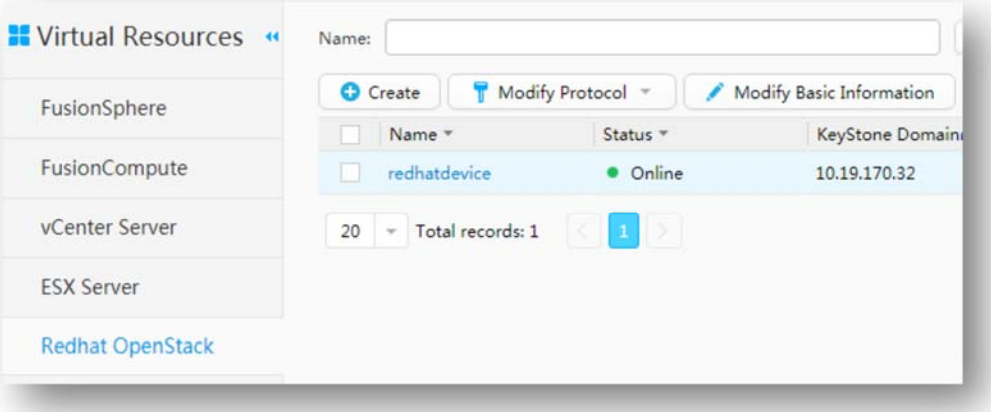
| Source NE | Source Port | Destination NE | Destination Port | Status | Type | Bandwidth | Operation |
|---|---|---|---|---|---|---|---|
| HUAWEI | GigabitEthernet0/0/33 | switch-114 | GigabitEthernet0/0/27 | Critical Fault | Layer 2 Link | 1000 | |

eSight Operations Guide Issue 08 (2018-08-28) at 942-944.

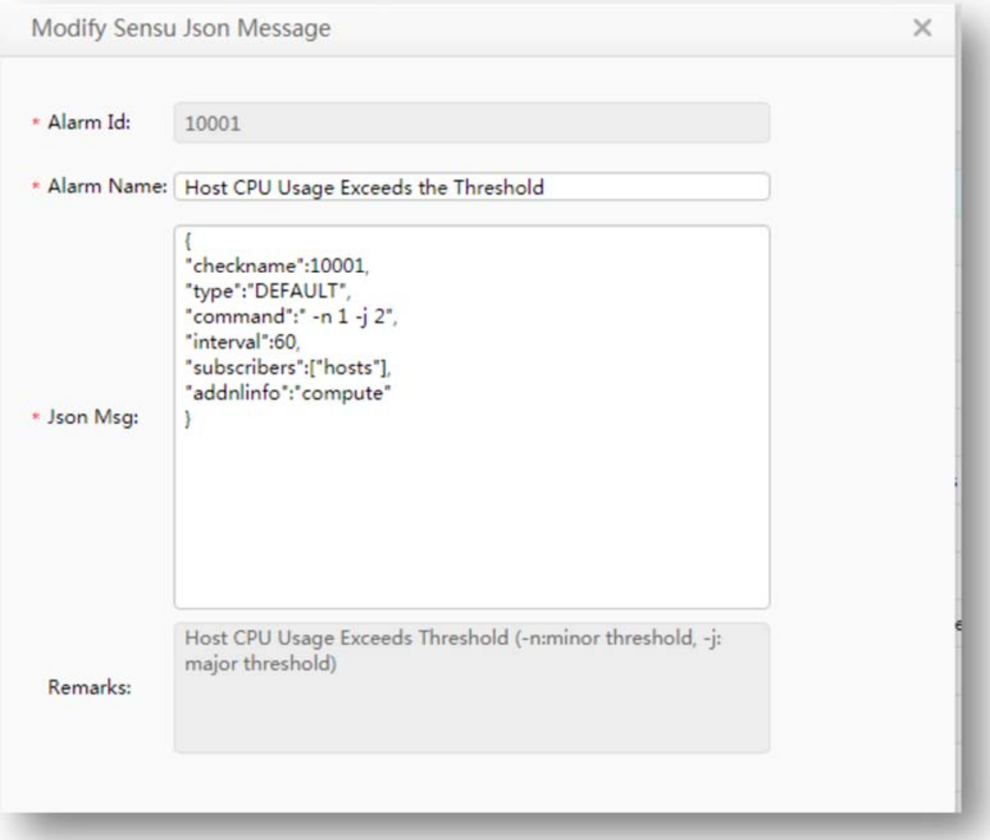
In Virtual Resource Management, the network map may change a different color indicative of a vulnerability, for example, when Performance Thresholds are met or approached:

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | <br>Click Performance Threshold Settings on the resource list page to set the monitoring thresholds, including the normal status (in green), risk (in orange), and high risk (in red) for indicators such as CPU utilization and memory utilization.<br><br>eSight Operations Guide Issue 08 (2018-08-28) at 966-67 (describing Performance Thresholds for FusionSphere host and VMs); *accord id.* at 982-83 (describing same for FusionCompute); *id.* at 997-98 (vCenter Server); *id.* at 1014-15 (RedHat Openstack).<br><br>Further, certain user-defined Alarm thresholds may be configured in Virtual Resources Management. On information and belief, these alarm thresholds may also cause the network map to turn a different color indicative of a vulnerability.<br><br><br>Virtual Resource Configuration and Synchronization<br>- Configuring the global threshold and performance alarm threshold<br>Users can configure the alarm threshold and monitoring thresholds of KPIs such as the CPU usage and memory usage to flexibly monitor virtual resources.<br>- Synchronizing virtual resources<br>When the status of virtual resources managed by eSight changes, you can manually synchronize the changes or configure a synchronization policy to synchronize the changes at a scheduled time, ensuring that the virtual infrastructure information is updated in time.<br><br>eSight Operations Guide Issue 08 (2018-08-28) at 944.<br><br>Example thresholds within the RedHat OpenStack include: |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | 11.8 RedHat OpenStack Management<br>…<br>11.8.8 Alarm Threshold Configuration<br>Procedure to configure the Alarm threshold<br>According to System/Business requirement, Alarms threshold can be changed for specified alarms related to threshold. Procedure to configure the alarm threshold as below<br>Procedure:<br>Step 1 Login to eSight GUI with valid user. Go to Resource > Virtual Resource > RedHat OpenStack<br>Step 2 Select available openstack based on IP (as shown below in snapshot) |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | <br> Virtual Resources<br>FusionSphere<br>FusionCompute<br>vCenter Server<br>ESX Server<br>Redhat OpenStack<br>Name:<br>Create<br>Modify Protocol<br>Modify Basic Information<br>Name<br>Status<br>KeyStone Domain<br>redhatdevice<br>● Online<br>10.19.170.32<br>20<br>Total records: 1<br>1<br>Step 3 Select an Openstack, Go to Settings > HTTPS Protocol Setting > Sensu Parameter Setting >Search Alarm based on Alarm ID or Name or JSON Msg.<br>Step 4 Select an alarm, set threshold of Alarms limit. Select Edit icon on GUI On operation column. Click on Edit option and set the threshold parameters like below, description of command to set threshold is as below |

***Harris Corporation v. Huawei, et al* – Case No. 2:18-cv-439**
**Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)**
**Exhibit A – U.S. Patent No. 6,535,227 ('227) – Claims 1-6, 8-13, 15-20, 22, 24**

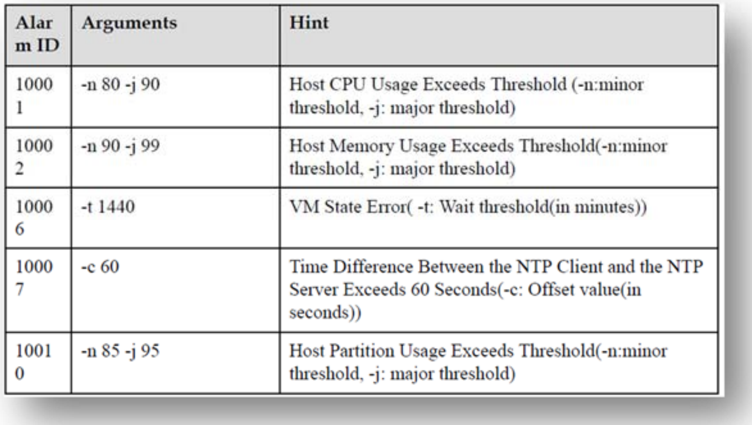
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | <br> <br>* Alarm Id: 10001<br>* Alarm Name: Host CPU Usage Exceeds the Threshold<br>* Json Msg: {<br>"checkname":10001,<br>"type":"DEFAULT",<br>"command":" -n 1 -j 2",<br>"interval":60,<br>"subscribers":["hosts"],<br>"addnlinfo":"compute"<br>}<br>Remarks: Host CPU Usage Exceeds Threshold (-n:minor threshold, -j: major threshold)<br>NOTE |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|

- interval - time gap between the alarm syncronization in seconds
- There are only for some alarm, can set threshold limit like CPU usage, memory usage, I/O Delay of the Storage Disk Is Too Long, Storage Usage Exceeds the Threshold and so on.

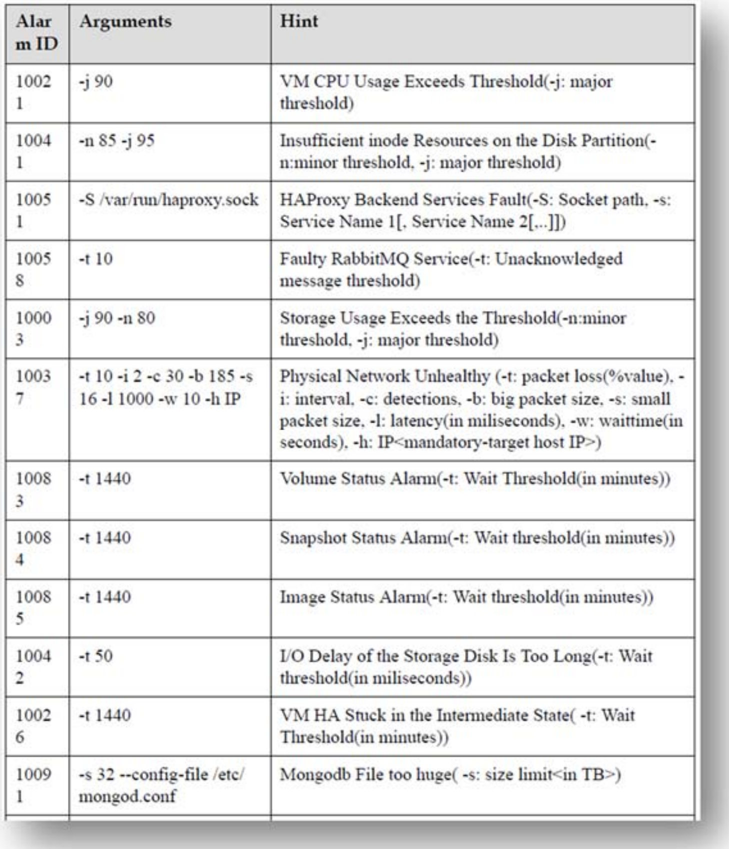
-n represent minor threshold limit like 99 is mentioned, also –j represent major threshold limit 100. Likewise all the limits will be set.

List of Alarm ID and Configuration parameter below

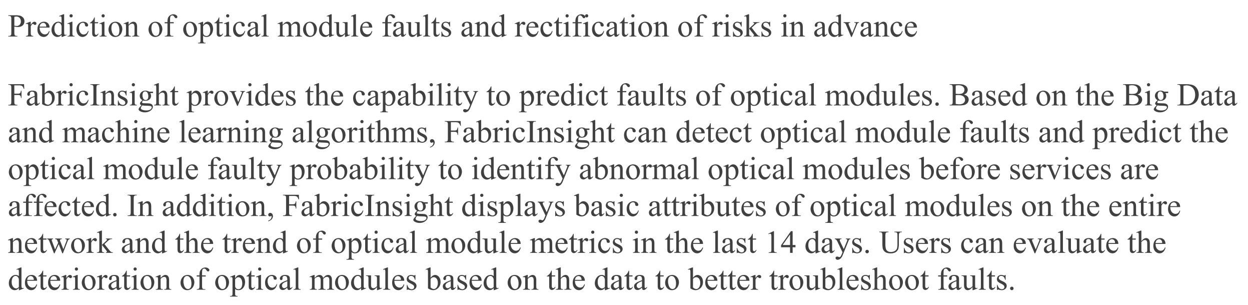


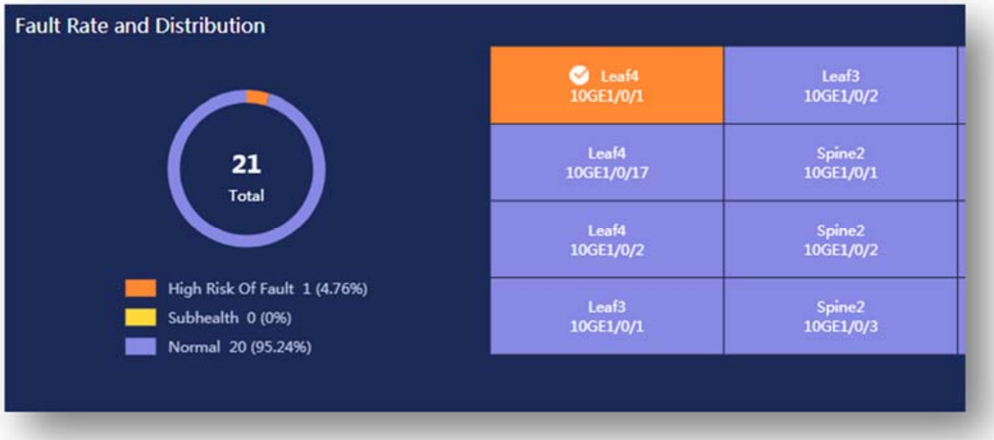
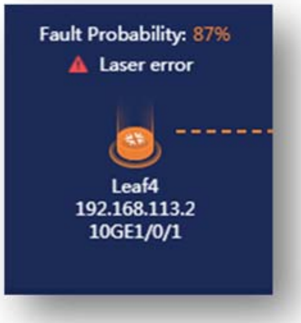
| Alarm ID | Arguments | Hint |
|---|---|---|
| 10001 | -n 80 -j 90 | Host CPU Usage Exceeds Threshold (-n:minor threshold, -j: major threshold) |
| 10002 | -n 90 -j 99 | Host Memory Usage Exceeds Threshold(-n:minor threshold, -j: major threshold) |
| 10006 | -t 1440 | VM State Error( -t: Wait threshold(in minutes)) |
| 10007 | -c 60 | Time Difference Between the NTP Client and the NTP Server Exceeds 60 Seconds(-c: Offset value(in seconds)) |
| 10010 | -n 85 -j 95 | Host Partition Usage Exceeds Threshold(-n:minor threshold, -j: major threshold) |

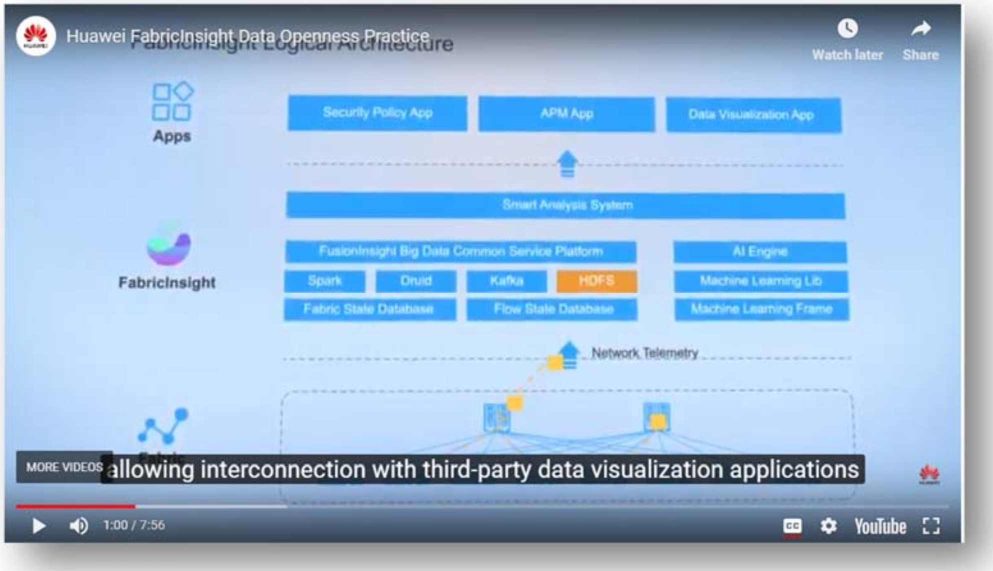
*Harris Corporation v. Huawei, et al* – **Case No. 2:18-cv-439**
**Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)**
**Exhibit A – U.S. Patent No. 6,535,227 ('227) – Claims 1-6, 8-13, 15-20, 22, 24**

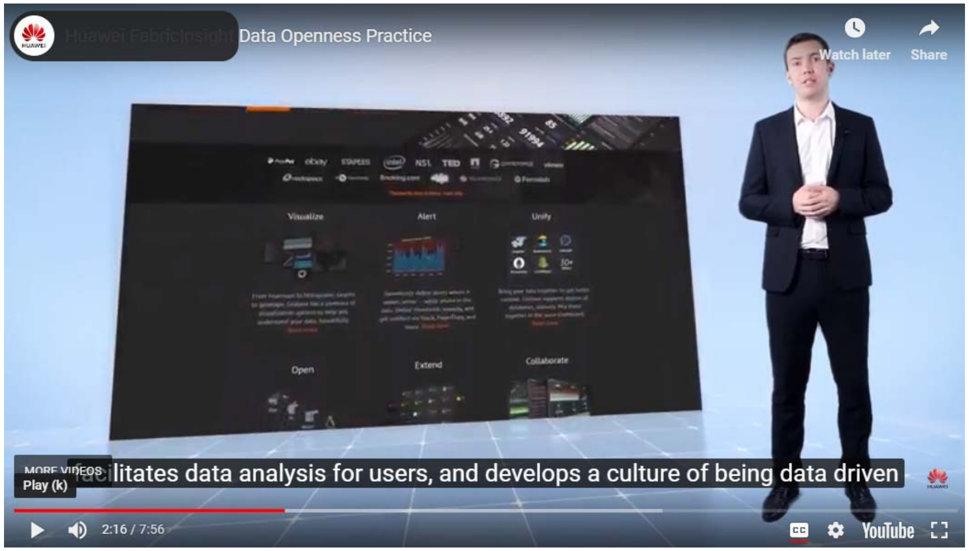
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | <br>eSight Operations Guide Issue 08 (2018-08-28) at 1019-1022 (see also additional alarms and thresholds contained in documentation) |

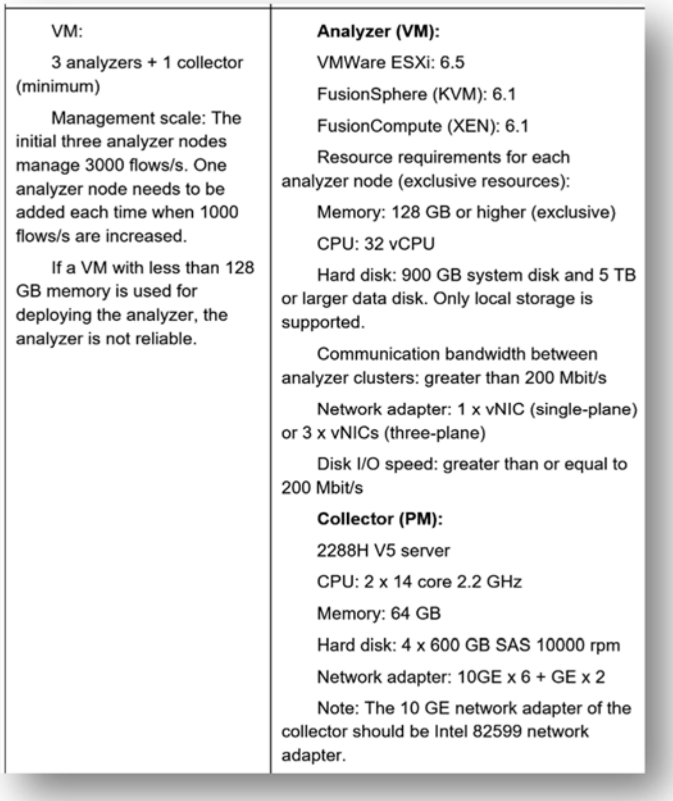
| Alarm ID | Arguments | Hint |
|---|---|---|
| 10021 | -j 90 | VM CPU Usage Exceeds Threshold(-j: major threshold) |
| 10041 | -n 85 -j 95 | Insufficient inode Resources on the Disk Partition(-n:minor threshold, -j: major threshold) |
| 10051 | -S /var/run/haproxy.sock | HAProxy Backend Services Fault(-S: Socket path, -s: Service Name 1[, Service Name 2[...]]) |
| 10058 | -t 10 | Faulty RabbitMQ Service(-t: Unacknowledged message threshold) |
| 10003 | -j 90 -n 80 | Storage Usage Exceeds the Threshold(-n:minor threshold, -j: major threshold) |
| 10037 | -t 10 -i 2 -c 30 -b 185 -s 16 -l 1000 -w 10 -h IP | Physical Network Unhealthy (-t: packet loss(%value), -i: interval, -c: detections, -b: big packet size, -s: small packet size, -l: latency(in miliseconds), -w: waittime(in seconds), -h: IP<mandatory-target host IP>) |
| 10083 | -t 1440 | Volume Status Alarm(-t: Wait Threshold(in minutes)) |
| 10084 | -t 1440 | Snapshot Status Alarm(-t: Wait threshold(in minutes)) |
| 10085 | -t 1440 | Image Status Alarm(-t: Wait threshold(in minutes)) |
| 10042 | -t 50 | I/O Delay of the Storage Disk Is Too Long(-t: Wait threshold(in miliseconds)) |
| 10026 | -t 1440 | VM HA Stuck in the Intermediate State( -t: Wait Threshold(in minutes)) |
| 10091 | -s 32 --config-file /etc/mongod.conf | Mongodb File too huge( -s: size limit<in TB>) |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | In another example, on the FabricInsight interface, selected portions of the network map turn a different color indicative of a vulnerability that has been established for that portion of the network after a security posture of the network has been established by correlating a system object model database that supports information data requirements of disparate network vulnerability analysis programs with any data results obtained from the programs.<br>For example, FabricInsight detects vulnerabilities:<br><br>Prediction of optical module faults and rectification of risks in advance<br>FabricInsight provides the capability to predict faults of optical modules. Based on the Big Data and machine learning algorithms, FabricInsight can detect optical module faults and predict the optical module faulty probability to identify abnormal optical modules before services are affected. In addition, FabricInsight displays basic attributes of optical modules on the entire network and the trend of optical module metrics in the last 14 days. Users can evaluate the deterioration of optical modules based on the data to better troubleshoot faults. |

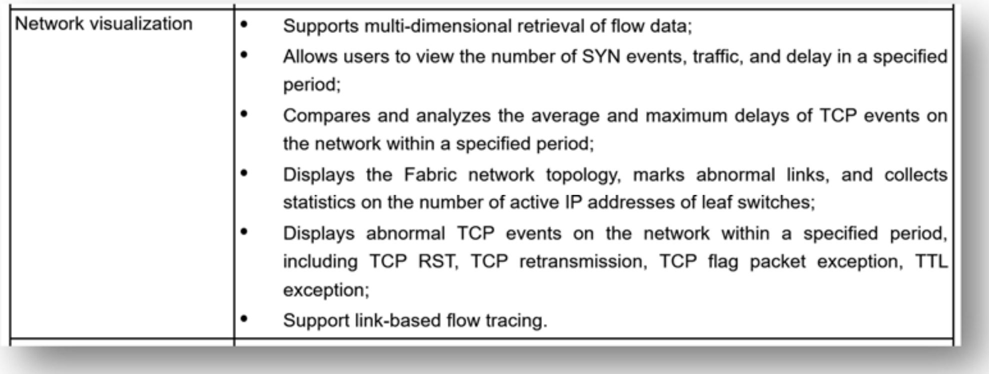
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | <br>Fault Rate and Distribution<br>21 Total<br>🟧 High Risk Of Fault 1 (4.76%)<br>🟨 Subhealth 0 (0%)<br>🟪 Normal 20 (95.24%)<br>Leaf4 10GE1/0/1 · Leaf3 10GE1/0/2<br>Leaf4 10GE1/0/17 · Spine2 10GE1/0/1<br>Leaf4 10GE1/0/2 · Spine2 10GE1/0/2<br>Leaf3 10GE1/0/1 · Spine2 10GE1/0/3<br><br>Fault Probability: 87%<br>⚠ Laser error<br>Leaf4<br>192.168.113.2<br>10GE1/0/1<br>Huawei FabricInsight Datasheet at 5-6. |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | FabricInsights also supports various third-party applications to determine network vulnerabilities, for example:<br>"As well as collecting and then processing data to analyze and then display, FabricInsight is very open, allowing interconnection with third-party data visualization applications"<br><br>Huawei FabricInsight Data Openness Practice<br>allowing interconnection with third-party data visualization applications<br> FabricInsight Logical Architecture<br>Watch later<br>Share<br>Apps<br>Security Policy App<br>APM App<br>Data Visualization App<br>Smart Analysis System<br>FabricInsight<br>FusionInsight Big Data Common Service Platform<br>Spark<br>Druid<br>Kafka<br>HDFS<br>Fabric State Database<br>Flow State Database<br>AI Engine<br>Machine Learning Lib<br>Machine Learning Frame<br>Network Telemetry<br>MORE VIDEOS<br>1:00 / 7:56<br>YouTube<br>https://support.huawei.com/enterprise/en/doc/EDOC1100025096 |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | "FabricInsights integrates with Grafana. Grafana is an open source software that displays data from multiple platforms facilitates data analysis for users, and develops a culture of being data driven."<br> Huawei FabricInsight Data Openness Practice<br>Watch later<br>Share<br>Visualize<br>Alert<br>Unify<br>Open<br>Extend<br>Collaborate<br>MORE VIDEOS<br>Play (k)<br>2:16 / 7:56<br>YouTube<br>facilitates data analysis for users, and develops a culture of being data driven<br>https://support.huawei.com/enterprise/en/doc/EDOC1100025096<br>FabricInsight supports hardware configurations of physical servers and VMs. In the VM implementation, the Analyzer uses disparate network vulnerability analysis programs, for example, VMWare ESXi, FusionSphere, FusionCompute: |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | <br>VM:<br>3 analyzers + 1 collector (minimum)<br>Management scale: The initial three analyzer nodes manage 3000 flows/s. One analyzer node needs to be added each time when 1000 flows/s are increased.<br>If a VM with less than 128 GB memory is used for deploying the analyzer, the analyzer is not reliable.<br>**Analyzer (VM):**<br>VMWare ESXi: 6.5<br>FusionSphere (KVM): 6.1<br>FusionCompute (XEN): 6.1<br>Resource requirements for each analyzer node (exclusive resources):<br>Memory: 128 GB or higher (exclusive)<br>CPU: 32 vCPU<br>Hard disk: 900 GB system disk and 5 TB or larger data disk. Only local storage is supported.<br>Communication bandwidth between analyzer clusters: greater than 200 Mbit/s<br>Network adapter: 1 x vNIC (single-plane) or 3 x vNICs (three-plane)<br>Disk I/O speed: greater than or equal to 200 Mbit/s<br>**Collector (PM):**<br>2288H V5 server<br>CPU: 2 x 14 core 2.2 GHz<br>Memory: 64 GB<br>Hard disk: 4 x 600 GB SAS 10000 rpm<br>Network adapter: 10GE x 6 + GE x 2<br>Note: The 10 GE network adapter of the collector should be Intel 82599 network adapter.<br>Huawei FabricInsight Datasheet at 9-10. *See also id.* at 12 (identifying VMWare ESXi, FusionSphere, FusionCompute as software for virtual machines) |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | Vulnerabilities may be displayed in the network topology: |

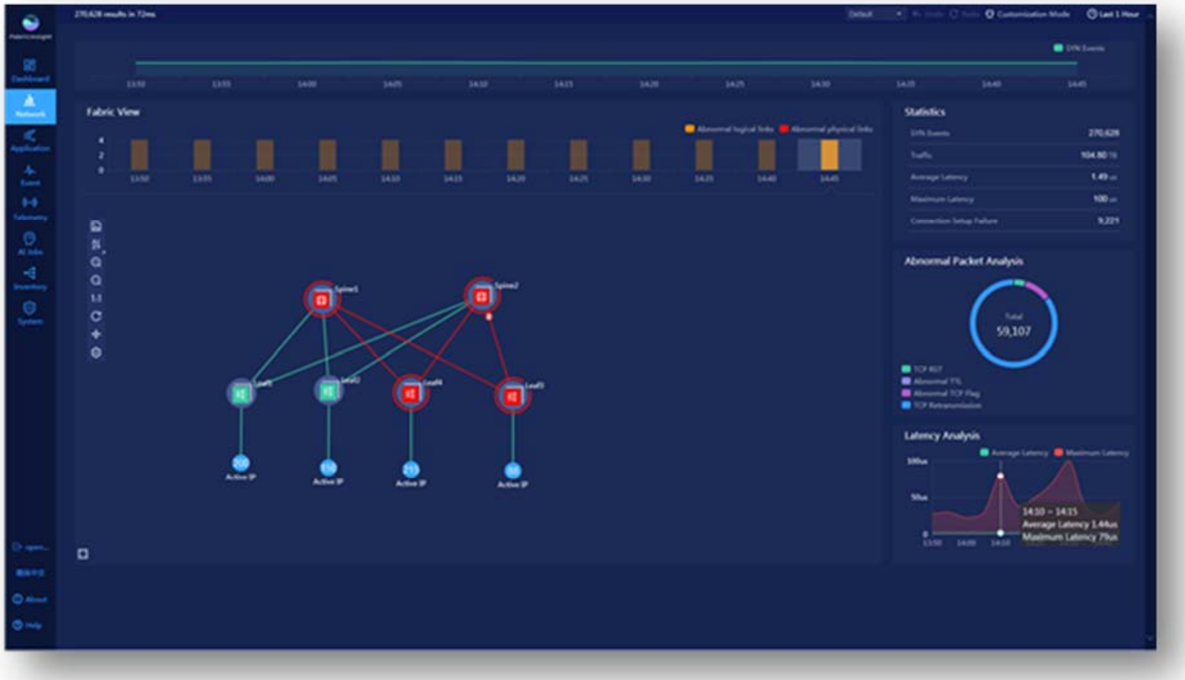


| Network visualization | • Supports multi-dimensional retrieval of flow data;<br>• Allows users to view the number of SYN events, traffic, and delay in a specified period;<br>• Compares and analyzes the average and maximum delays of TCP events on the network within a specified period;<br>• Displays the Fabric network topology, marks abnormal links, and collects statistics on the number of active IP addresses of leaf switches;<br>• Displays abnormal TCP events on the network within a specified period, including TCP RST, TCP retransmission, TCP flag packet exception, TTL exception;<br>• Support link-based flow tracing. |
|---|---|

Huawei FabricInsight Datasheet at 9.

> Live network quality evaluation and proactive detection of abnormal network flows
>
> The FabricInsight provides the network view, performs intelligent analysis of TCP flow status and detects abnormal flows based on big data, displays network quality in real time through indicators such as delay and traffic, and quickly identifies and analyzes abnormal flows on the network.

*Harris Corporation v. Huawei, et al* – **Case No. 2:18-cv-439**
**Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)**
**Exhibit A – U.S. Patent No. 6,535,227 ('227) – Claims 1-6, 8-13, 15-20, 22, 24**

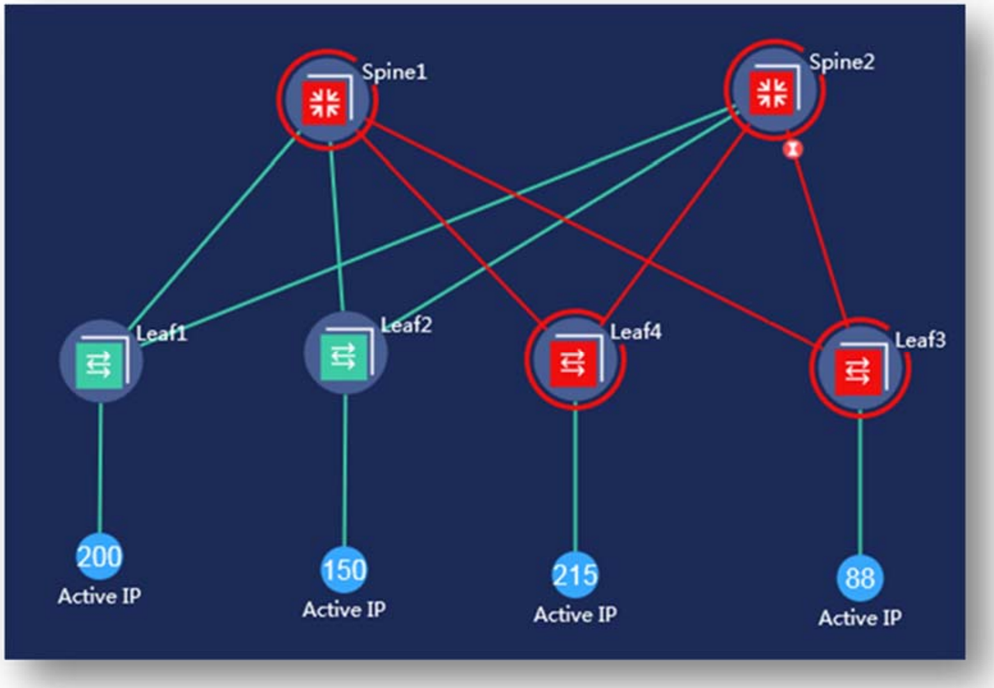
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |  |

270,628 results in 72ms

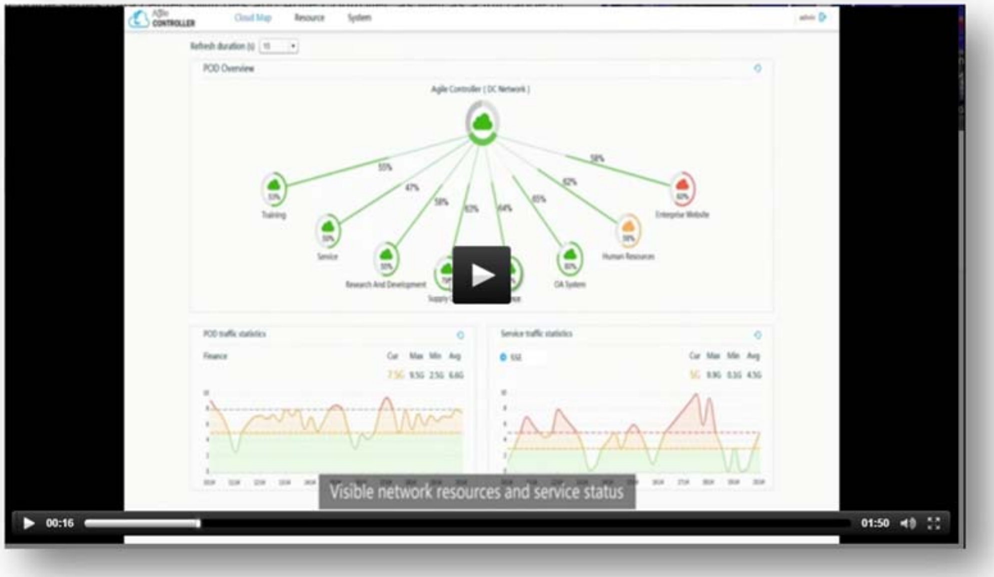
Statistics

| | |
|---|---|
| SYN Events | 270,628 |
| Traffic | 104.80 TB |
| Average Latency | 1.49 us |
| Maximum Latency | 100 us |
| Connection Setup Failure | 9,221 |

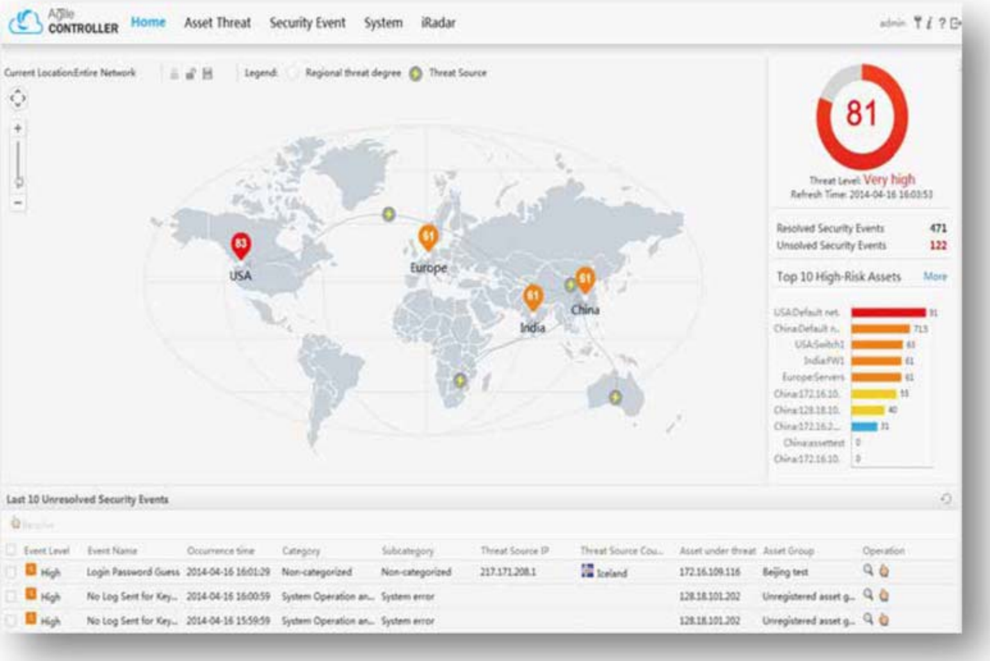
14:10 – 14:15
Average Latency 1.44us
Maximum Latency 79us

| '227 Patent Claim 1 | Infringement By Huawei Corporation |
|---|---|
| | <br> Spine1<br>Spine2<br>Leaf1<br>Leaf2<br>Leaf4<br>Leaf3<br>200<br>Active IP<br>150<br>Active IP<br>215<br>Active IP<br>88<br>Active IP<br>Huawei FabricInsight Datasheet at 3-4.<br>Further, the Agile Controller network map turns a different color indicative of a vulnerability that has been established for that portion of the network after a security posture of the network has been established by correlating a system object model database that supports information data requirements of disparate network vulnerability analysis programs with any data results obtained from the programs. |

*Harris Corporation v. Huawei, et al* – Case No. 2:18-cv-439
Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)
Exhibit A – U.S. Patent No. 6,535,227 ('227) – Claims 1-6, 8-13, 15-20, 22, 24

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | For example, as shown below, network icons turn a different color to indicate vulnerability:<br><br> Agile CONTROLLER<br>Cloud Map<br>Resource<br>System<br>admin<br>Refresh duration (s)<br>10<br>POD Overview<br>Agile Controller ( DC Network )<br>55%<br>47%<br>58%<br>63%<br>64%<br>65%<br>62%<br>58%<br>Training<br>Service<br>Research And Development<br>Supply<br>OA System<br>Human Resources<br>Enterprise Website<br>POD traffic statistics<br>Finance<br>Cur Max Min Avg<br>7.5G 9.5G 2.5G 6.6G<br>Service traffic statistics<br>Cur Max Min Avg<br>5G 8.9G 0.3G 4.5G<br>00:16<br>01:50<br>Visible network resources and service status<br>Huawei Video: *Cloud Fabric: Huawei and VMWare Innovate* (e.huawei.com/en-US/videos/global/older/hw_362493) (Huawei and VMWare co-operate on an SDN data center networking solution) at 0:16.<br>Security Situation Display, Providing the Basis for Proactive Defense<br>• Divides the entire network into several areas and marks them with different colors based on the security view of the entire network. |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | • Identifies Top N risky assets on the entire network and evaluates the security level of the network, helping users quickly obtain the network security status. |



Resolved Security Events 471
Unsolved Security Events 122

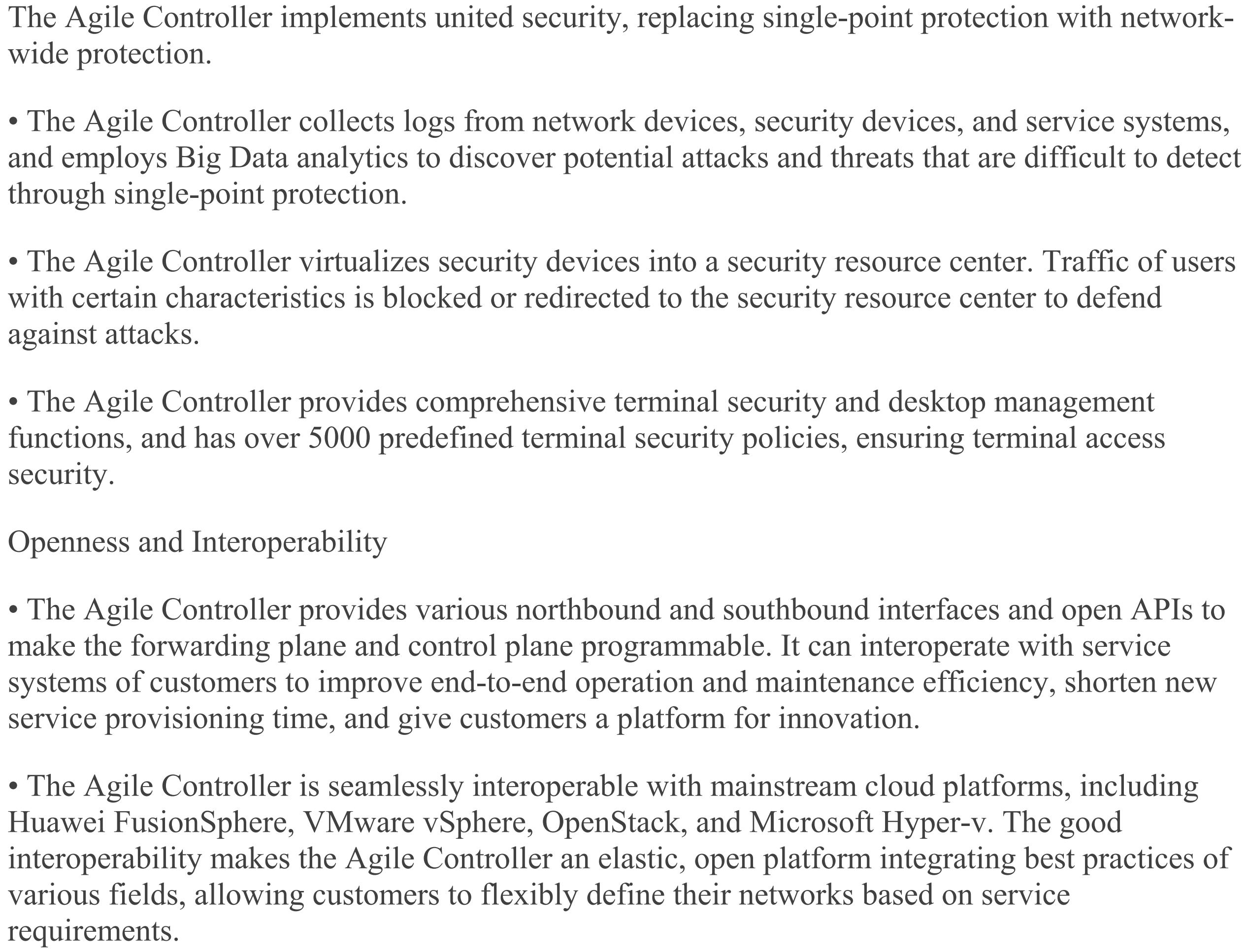
Top 10 High-Risk Assets More

Last 10 Unresolved Security Events

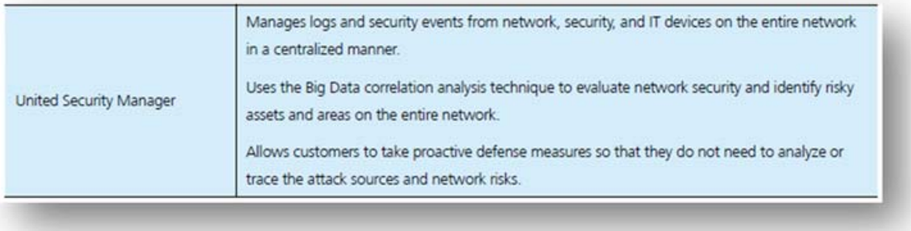
| Event Level | Event Name | Occurrence time | Category | Subcategory | Threat Source IP | Threat Source Cou... | Asset under threat | Asset Group | Operation |
|---|---|---|---|---|---|---|---|---|---|
| High | Login Password Guess | 2014-04-16 16:01:29 | Non-categorized | Non-categorized | 217.171.208.1 | Iceland | 172.16.109.116 | Beijing test | |
| High | No Log Sent for Key... | 2014-04-16 16:00:59 | System Operation an... | System error | | | 128.18.101.202 | Unregistered asset g... | |
| High | No Log Sent for Key... | 2014-04-16 15:59:59 | System Operation an... | System error | | | 128.18.101.202 | Unregistered asset g... | |

The Agile Controller interfaces with various network vulnerability analysis programs and devices to determine vulnerabilities and a security posture of the network.

Network-wide United Security

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | <br>The Agile Controller implements united security, replacing single-point protection with network-wide protection.<br>• The Agile Controller collects logs from network devices, security devices, and service systems, and employs Big Data analytics to discover potential attacks and threats that are difficult to detect through single-point protection.<br>• The Agile Controller virtualizes security devices into a security resource center. Traffic of users with certain characteristics is blocked or redirected to the security resource center to defend against attacks.<br>• The Agile Controller provides comprehensive terminal security and desktop management functions, and has over 5000 predefined terminal security policies, ensuring terminal access security.<br>Openness and Interoperability<br>• The Agile Controller provides various northbound and southbound interfaces and open APIs to make the forwarding plane and control plane programmable. It can interoperate with service systems of customers to improve end-to-end operation and maintenance efficiency, shorten new service provisioning time, and give customers a platform for innovation.<br>• The Agile Controller is seamlessly interoperable with mainstream cloud platforms, including Huawei FusionSphere, VMware vSphere, OpenStack, and Microsoft Hyper-v. The good interoperability makes the Agile Controller an elastic, open platform integrating best practices of various fields, allowing customers to flexibly define their networks based on service requirements.<br>HUAWEI Agile Controller Full Product Datasheet 1 at 6. |

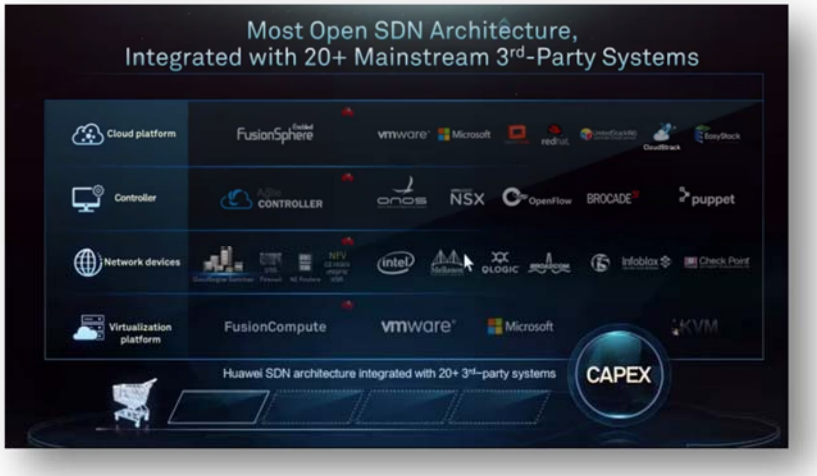
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | |



| | |
|---|---|
| United Security Manager | Manages logs and security events from network, security, and IT devices on the entire network in a centralized manner.<br>Uses the Big Data correlation analysis technique to evaluate network security and identify risky assets and areas on the entire network.<br>Allows customers to take proactive defense measures so that they do not need to analyze or trace the attack sources and network risks. |

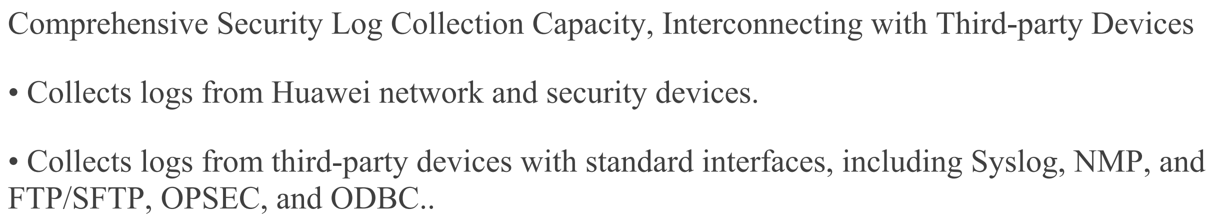
Agile Controller Full Product Datasheet at 7.

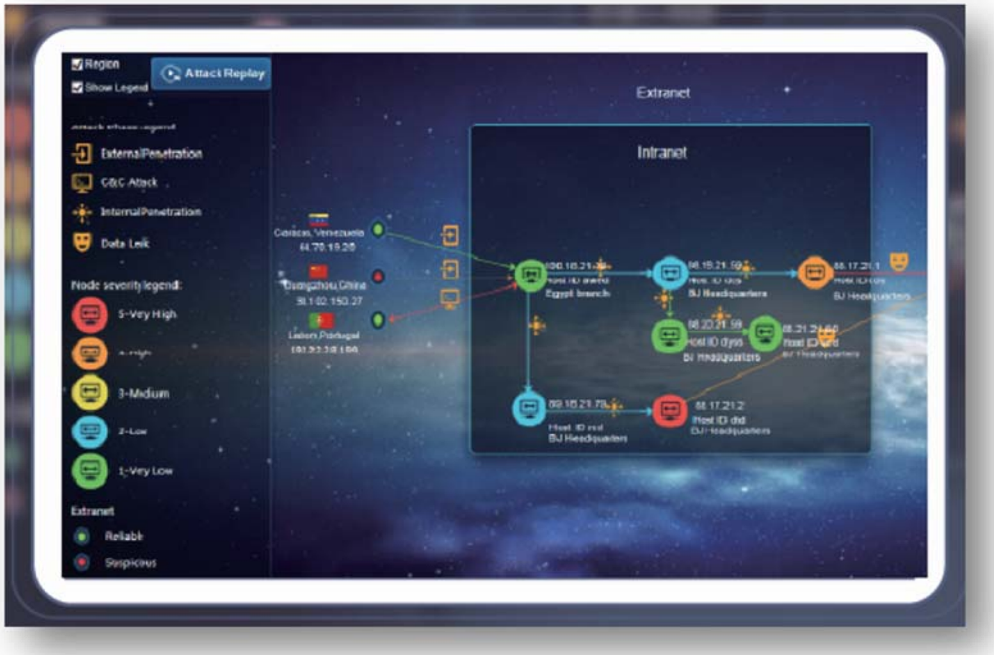
Agile Controller SDN Integrates with 20+ Mainstream 3rd-Party systems which can also provide network vulnerability analysis:

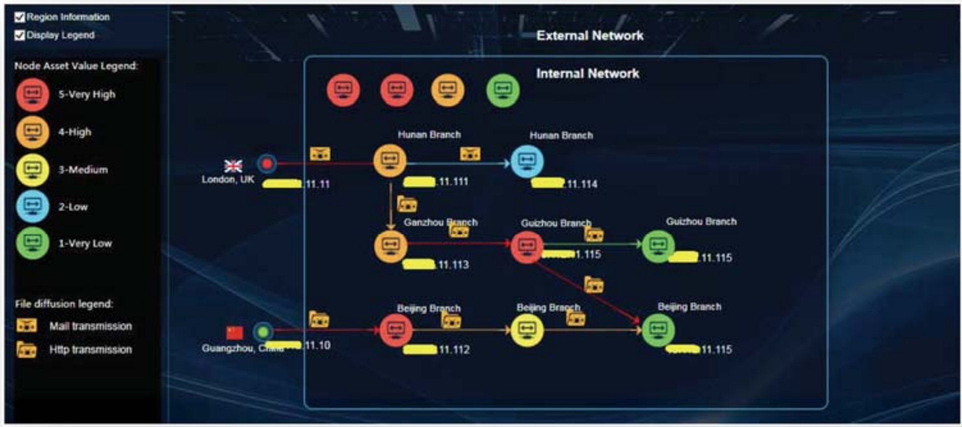


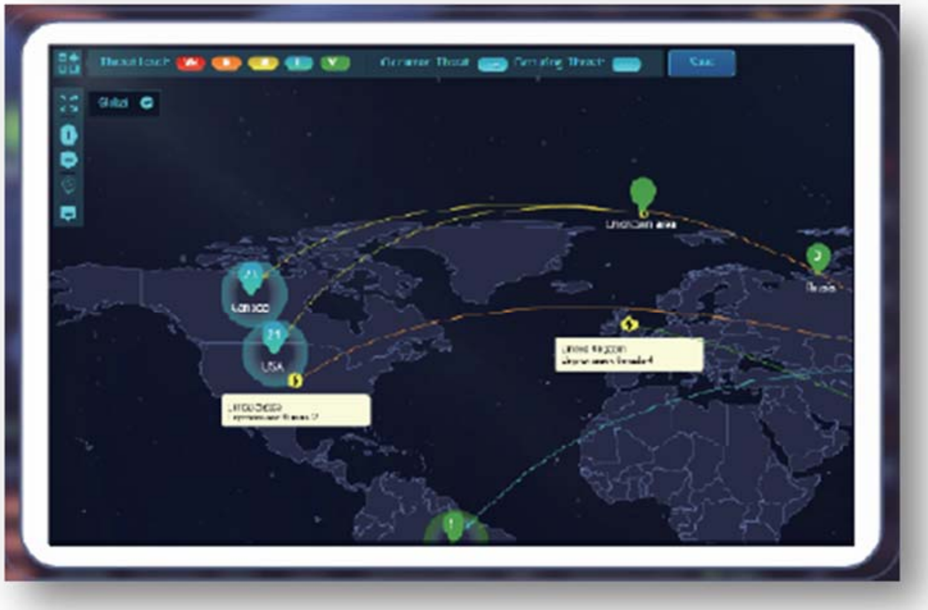
Most Open SDN Architecture, Integrated with 20+ Mainstream 3rd-Party Systems

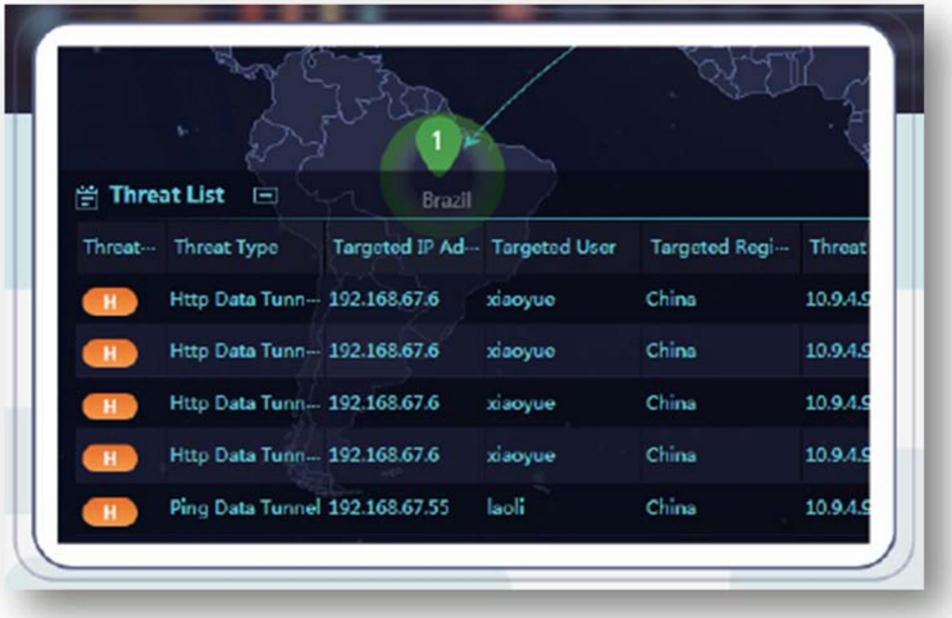
Huawei SDN architecture integrated with 20+ 3rd-party systems

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | Video: *Huawei CloudFabric Data Center Network Solution* at 2:21 (e.huawei.com/en-US/videos/global/2016/201611161014) (Huawei CloudFabric Data Center Network Solution enables agile deployment, refined OM, open ecosystem, and intelligent security protection, which allows for faster service deployment and provisioning, quick fault location, and improved network security.); *See also*, discussion above regarding FusionSphere, VMware vSphere, OpenStack vulnerability assessment tools.<br>See also:<br><br>Comprehensive Security Log Collection Capacity, Interconnecting with Third-party Devices<br>• Collects logs from Huawei network and security devices.<br>• Collects logs from third-party devices with standard interfaces, including Syslog, NMP, and FTP/SFTP, OPSEC, and ODBC..<br>Agile Controller Full Product Datasheet at 33.<br>Further, the Cybersecurity Intelligence System network map turns a different color indicative of a vulnerability that has been established for that portion of the network after a security posture of the network has been established by correlating a system object model database that supports information data requirements of disparate network vulnerability analysis programs with any data results obtained from the programs.<br>For example: |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |  ☑ Region<br>☑ Show Legend<br>Attack Replay<br>Extranet<br>Intranet<br>ExternalPenetration<br>C&C Attack<br>InternalPenetration<br>Data Leik<br>Node severity legend:<br>5-Very High<br>3-Medium<br>2-Low<br>1-Very Low<br>Extranet<br>Reliable<br>Suspicious<br>Caracas, Venezuela<br>Guangzhou China<br>Lisbon Portugal<br>Egypt branch<br>BJ Headquarters<br>Host ID did<br>The CIS visually displays multiple attack stages of advanced threats and asset information of key Nodes…<br>Huawei CIS Cybersecurity Intelligence System Product Description at 3.<br>*See also, e.g.,:* |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | <br> ☑ Region Information<br>☑ Display Legend<br>Node Asset Value Legend:<br>5-Very High<br>4-High<br>3-Medium<br>2-Low<br>1-Very Low<br>File diffusion legend:<br>Mail transmission<br>Http transmission<br>External Network<br>Internal Network<br>London, UK<br>[redacted].11.11<br>Hunan Branch<br>[redacted].11.111<br>Hunan Branch<br>[redacted].11.114<br>Ganzhou Branch<br>[redacted].11.113<br>Guizhou Branch<br>[redacted]1.115<br>Guizhou Branch<br>[redacted].11.115<br>Guangzhou, China<br>[redacted]11.10<br>Beijing Branch<br>[redacted].11.112<br>Beijing Branch<br>Beijing Branch<br>[redacted]11.115<br>Huawei CIS Cybersecurity Intelligence System Datasheet at 4.<br>Display of Security Posture on the Network Topology<br>The security posture awareness function maps network security threat events to a global topological map, uses the threat map to display threats and lately discovered threat events, and predicts and alerts the trend of network security. |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |  <br>Quick identification of highrisk assets and main threats<br>The CIS visually displays threats that target the internal users and assets of an enterprise, quickly identifies high-risk assets and main threats by categorizing users, asset groups, and threat events, and helps users specify regions to be secured and the solutions. |

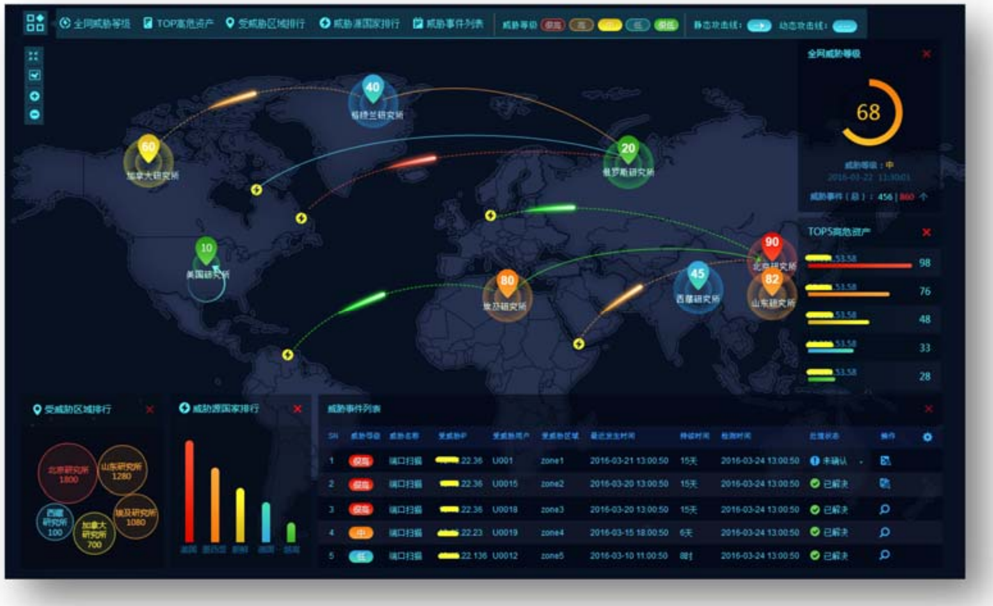
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |  |

Threat List

| Threat··· | Threat Type | Targeted IP Ad··· | Targeted User | Targeted Regi··· | Threat |
|---|---|---|---|---|---|
| H | Http Data Tunn··· | 192.168.67.6 | xiaoyue | China | 10.9.4.9 |
| H | Http Data Tunn··· | 192.168.67.6 | xiaoyue | China | 10.9.4.9 |
| H | Http Data Tunn··· | 192.168.67.6 | xiaoyue | China | 10.9.4.9 |
| H | Http Data Tunn··· | 192.168.67.6 | xiaoyue | China | 10.9.4.9 |
| H | Ping Data Tunnel | 192.168.67.55 | laoli | China | 10.9.4.9 |

Huawei CIS Cybersecurity Intelligence System Product Description at 3.

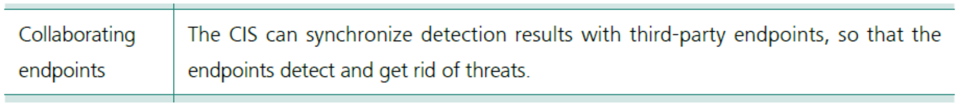
> Network visualization: Real-time awareness of security posture, enabling search and source tracing of PB-level data within seconds
>
> 1. Threat map: Clearly displays threats facing the enterprise network from all over the globe and the latest detected threat events on the threat map. This helps the O&M personnel to detect threats in a timely manner and predict network security trends.

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | 2. Key region-focused stage mode: Displays CIS security posture. A province, city, district, or county can be specified on a stage and the rest part of the world around the stage to show attack posture aiming at the region on the stage.<br><br> 全网威胁等级<br>TOP高危资产<br>受威胁区域排行<br>威胁源国家排行<br>威胁事件列表<br>威胁等级<br>静态攻击线：<br>动态攻击线：<br>40<br>20<br>60<br>10<br>80<br>45<br>90<br>82<br>68<br>98<br>76<br>48<br>33<br>28<br>北京研究所 1800<br>山东研究所 1280<br>西藏研究所 100<br>加拿大研究所 700<br>埃及研究所 1080<br>威胁事件列表<br>SN 威胁等级 威胁名称 受威胁IP 受威胁用户 受威胁区域 最近发生时间 持续时间 检测时间 处理状态 操作<br>1 很高 端口扫描 22.36 U001 zone1 2016-03-21 13:00:50 15天 2016-03-24 13:00:50 未确认<br>2 很高 端口扫描 22.36 U0015 zone2 2016-03-20 13:00:50 15天 2016-03-24 13:00:50 已解决<br>3 很高 端口扫描 22.36 U0018 zone3 2016-03-20 13:00:50 15天 2016-03-24 13:00:50 已解决<br>4 中 端口扫描 22.23 U0019 zone4 2016-03-15 18:00:50 6天 2016-03-24 13:00:50 已解决<br>5 低 端口扫描 22.136 U0012 zone5 2016-03-10 11:00:50 8时 2016-03-24 13:00:50 已解决<br>Global Security Posture Awareness<br>Huawei CIS Cybersecurity Intelligence System Datasheet at 6. |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | > As a Big Data security analysis system, the CIS dynamically monitors and analyzes APT security threats, visualizes the security posture of the entire network, and automatically blocks security threats. |

Huawei SDSec Security Solution Technical White Paper (for the DCN), Issue 01 (2017-07-20) at 8.

The CIS works with multiple third-party endpoints and disparate network vulnerability analysis programs to determine the security posture. For example:

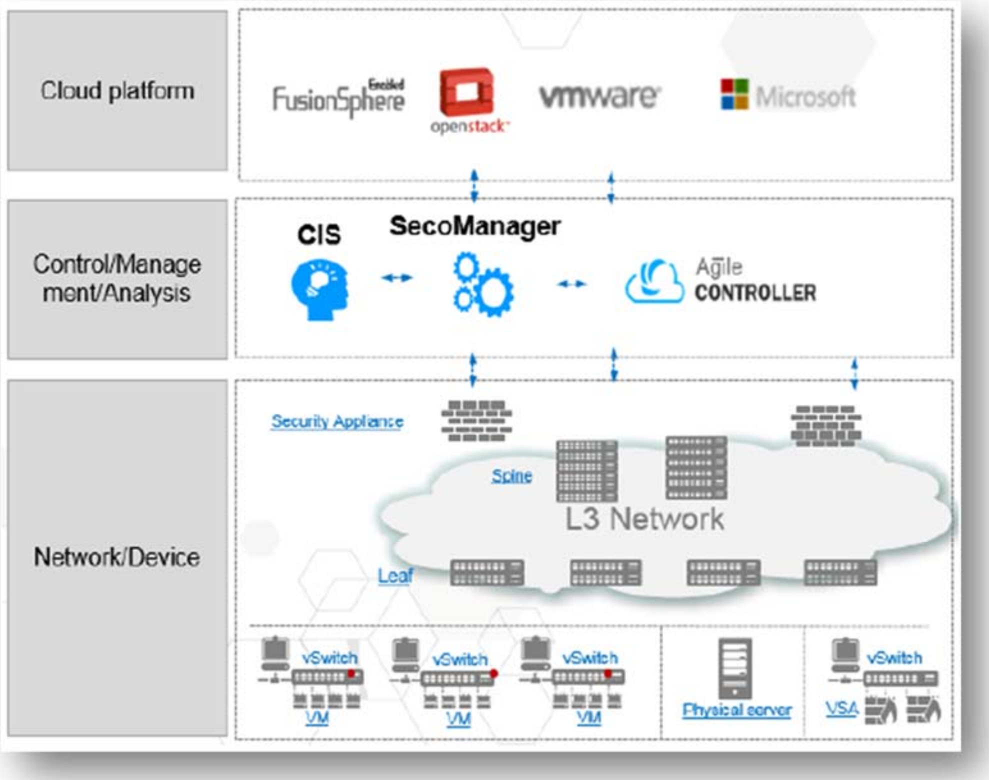


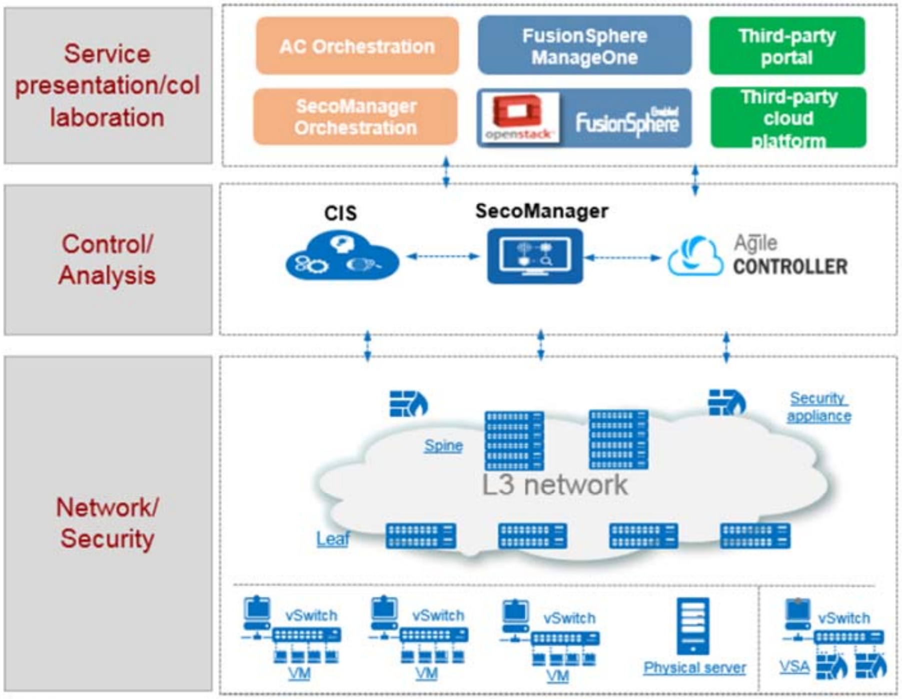
| | |
|---|---|
| Collaborating endpoints | The CIS can synchronize detection results with third-party endpoints, so that the endpoints detect and get rid of threats. |

Huawei CIS Cybersecurity Intelligence System Datasheet at 5.

CIS, as well as the Agile Controller further integrate with SDSec solutions, including SecoManager to establish a security posture of a network:

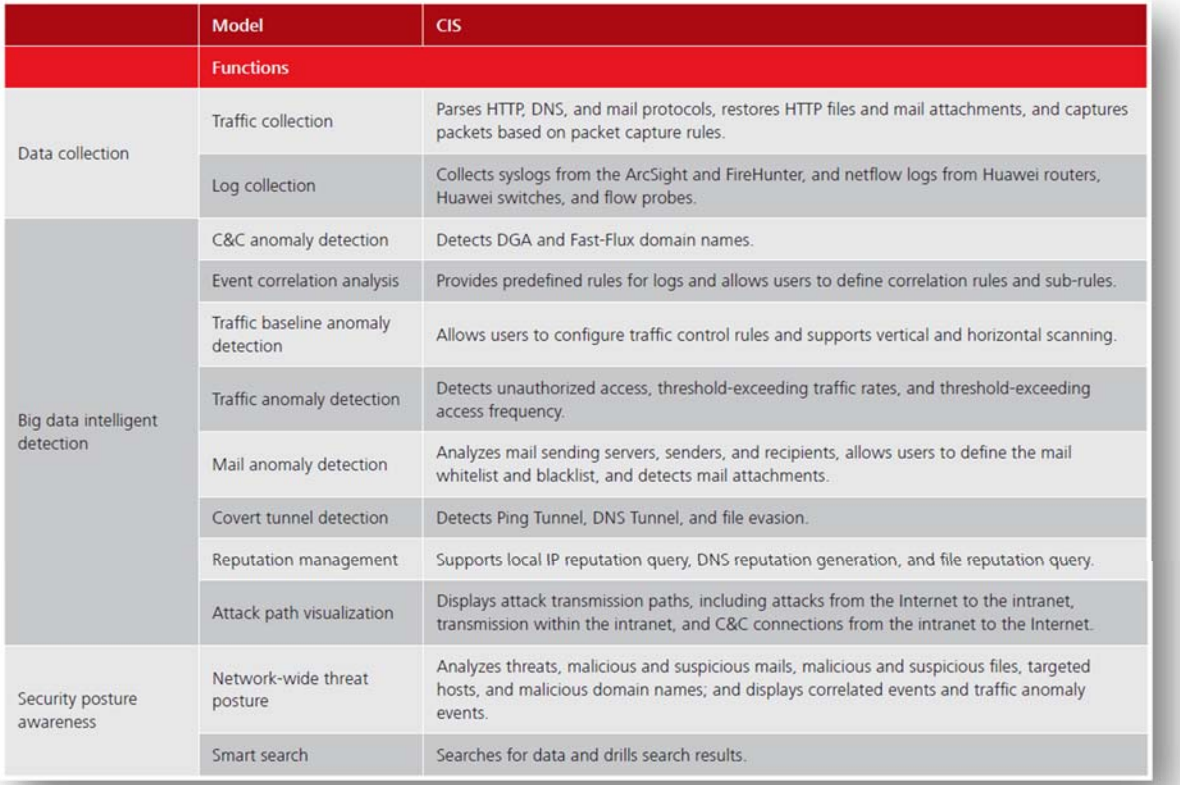
> Huawei SecoManager is a new-generation security controller oriented for enterprise and carrier data centers and markets. As a centralized security control plane, the SecoManager automatically orchestrates and delivers security configurations to implement automatic service delivery.
>
> The SecoManager can connect to a network controller (Agile Controller-DCN) and is compatible with a network management platform based on the Neutron service model. It provides diversified interconnection interfaces, including RPC and RESTful interfaces.
>
> The SecoManager can also interwork with a security analyzer (CIS) to provide quick response to threats and implement traffic-based intelligent policy simulation and tuning.

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |   Cloud platform<br>FusionSphere Enabled<br>openstack<br>vmware<br>Microsoft<br>Control/Management/Analysis<br>CIS<br>SecoManager<br>Agile CONTROLLER<br>Network/Device<br>Security Appliance<br>Spine<br>L3 Network<br>Leaf<br>vSwitch<br>VM<br>vSwitch<br>VM<br>vSwitch<br>VM<br>Physical server<br>vSwitch<br>VSA<br>Huawei SecoManager Security Controller Technical White Paper at 1. |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
|  | **Figure 2-1** Overall security architecture of DCN data centers<br><br> Service presentation/collaboration<br>AC Orchestration<br>FusionSphere ManageOne<br>Third-party portal<br>SecoManager Orchestration<br>openstack<br>FusionSphere<br>Third-party cloud platform<br>Control/ Analysis<br>CIS<br>SecoManager<br>Agile CONTROLLER<br>Network/ Security<br>Spine<br>Security appliance<br>L3 network<br>Leaf<br>vSwitch<br>VM<br>Physical server<br>VSA<br>Huawei SDSec Security Solution Technical White Paper (for the DCN), Issue 01 (2017-07-20) at 7.<br>Huawei SDSec introduces the security controller SecoManager. It can be integrated with software, hardware, and security components from Huawei and third parties, to enable centralized |

| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | security service orchestration and management. This will allow networks and security to be deeply intertwined and managed through security policies, effectively preventing threats. Using a security analyzer, SDSec offers intelligent threat detection and makes networks far less susceptible to attacks. It shifts protection from passive to active defense, helping to improve threat defense capabilities of enterprise and carrier networks. Intelligent threat response helps enterprises and carriers eliminate security risks and shift from node protection to network protection, ensuring minimal losses.<br>*Huawei Launches the SDSec Solution to Build a Proactive Network Defense System*, 2018/3/9 (https://e.huawei.com/en/news/global/2018/Huawei%20Launches%20the%20SDSec%20Solution%20to%20Build%20a%20Proactive%20Network%20Defense%20System)<br>Further, when user-defined thresholds and rules are met, CIS may indicate a vulnerability: |

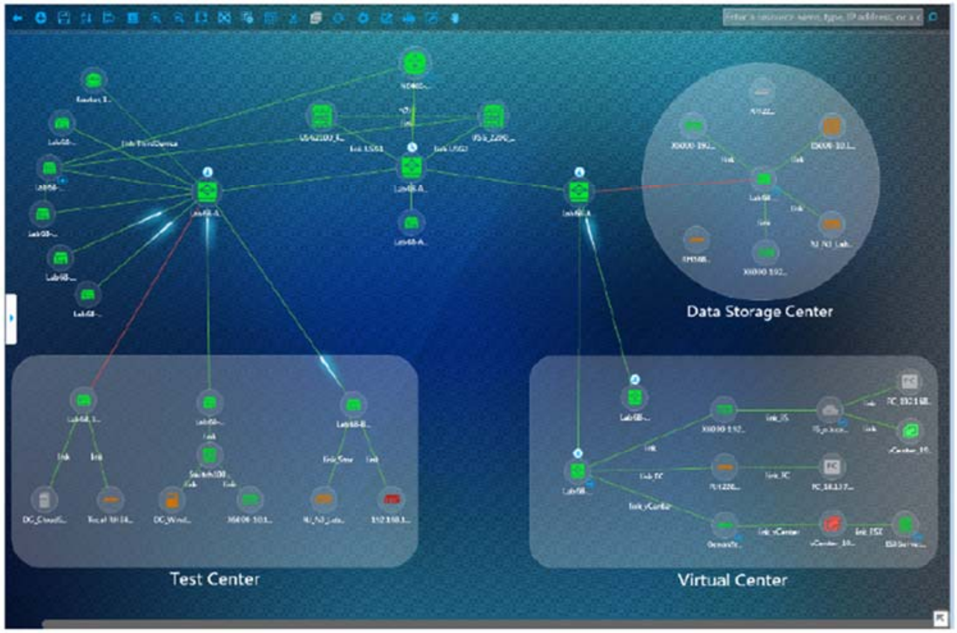
| '227 PATENT CLAIM 1 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
|  | See image and table below |

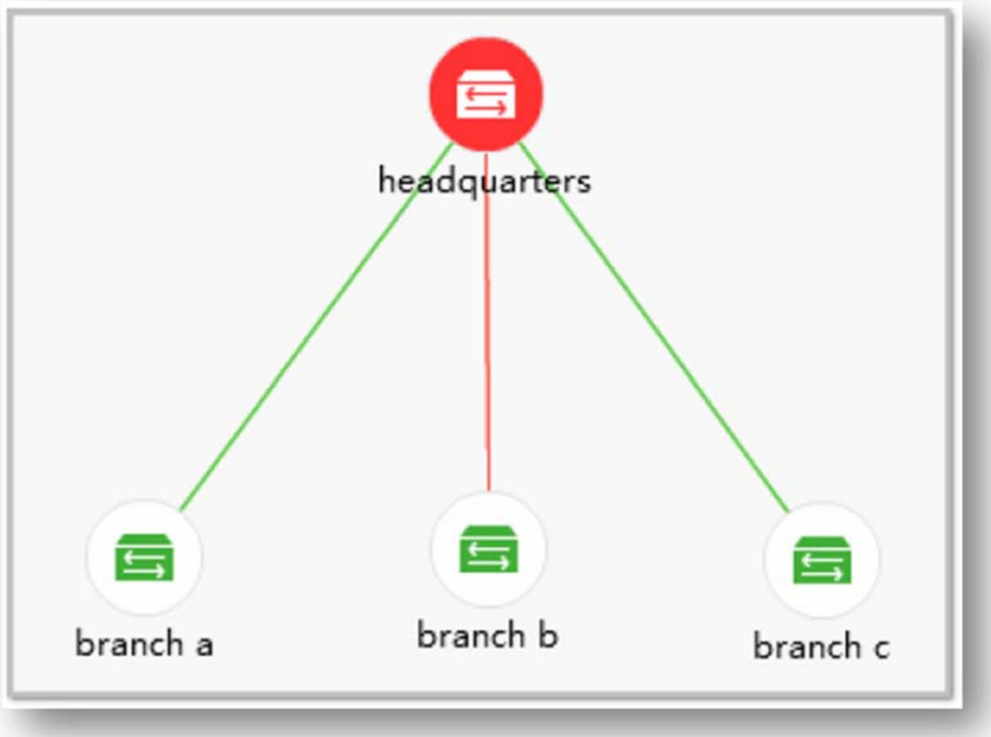


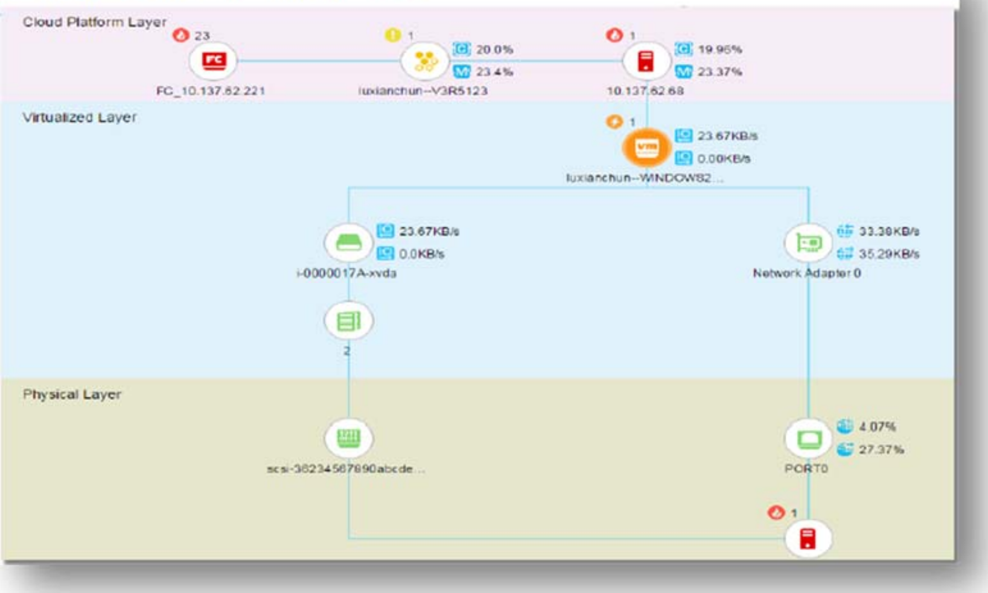
|  | Model | CIS |
|---|---|---|
|  | Functions |  |
| Data collection | Traffic collection | Parses HTTP, DNS, and mail protocols, restores HTTP files and mail attachments, and captures packets based on packet capture rules. |
|  | Log collection | Collects syslogs from the ArcSight and FireHunter, and netflow logs from Huawei routers, Huawei switches, and flow probes. |
| Big data intelligent detection | C&C anomaly detection | Detects DGA and Fast-Flux domain names. |
|  | Event correlation analysis | Provides predefined rules for logs and allows users to define correlation rules and sub-rules. |
|  | Traffic baseline anomaly detection | Allows users to configure traffic control rules and supports vertical and horizontal scanning. |
|  | Traffic anomaly detection | Detects unauthorized access, threshold-exceeding traffic rates, and threshold-exceeding access frequency. |
|  | Mail anomaly detection | Analyzes mail sending servers, senders, and recipients, allows users to define the mail whitelist and blacklist, and detects mail attachments. |
|  | Covert tunnel detection | Detects Ping Tunnel, DNS Tunnel, and file evasion. |
|  | Reputation management | Supports local IP reputation query, DNS reputation generation, and file reputation query. |
|  | Attack path visualization | Displays attack transmission paths, including attacks from the Internet to the intranet, transmission within the intranet, and C&C connections from the intranet to the Internet. |
| Security posture awareness | Network-wide threat posture | Analyzes threats, malicious and suspicious mails, malicious and suspicious files, targeted hosts, and malicious domain names; and displays correlated events and traffic anomaly events. |
|  | Smart search | Searches for data and drills search results. |

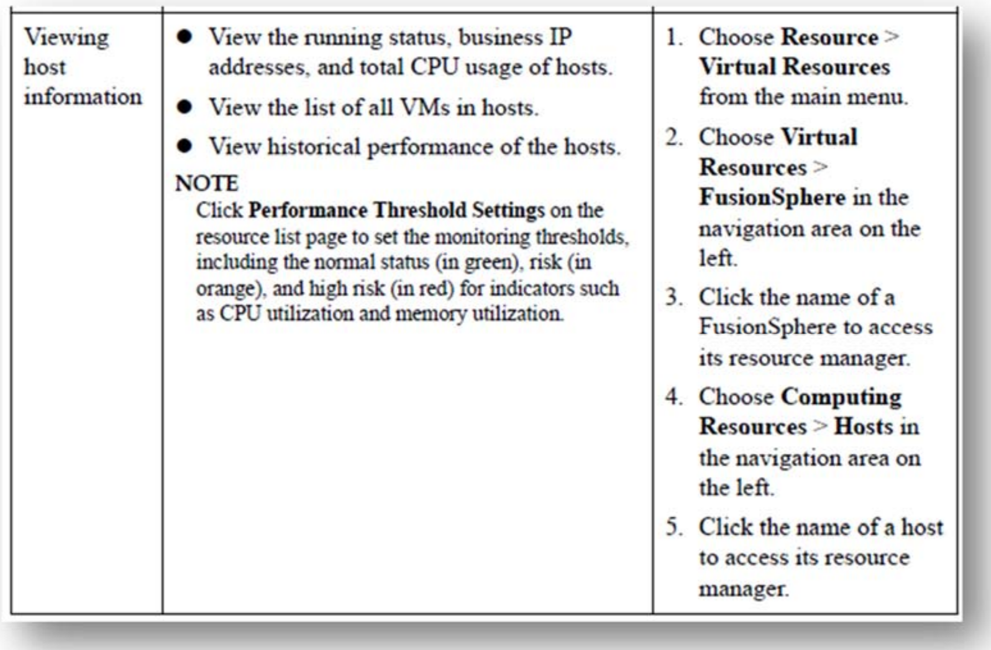
Huawei CIS Cybersecurity Intelligence System Brochure at 2.

| **'227 Patent Claim 2** | **Infringement By Huawei Corporation** |
|---|---|
| **2.** A graphical user interface according to claim 1, wherein respective network elements turn a different color indicative of a vulnerable network node. | The Huawei '227 Patent Accused Instrumentalities infringe this claim. *See* Claim 1.<br>Further, respective network elements turn a different color indicative of a vulnerable network node.<br>For example, in the eSight topology view, network elements change color when a node is vulnerable:<br>The eSight provides various alarm monitoring methods and multidimensional alarm data statistics.<br>…<br>- Monitor alarms on a topology |

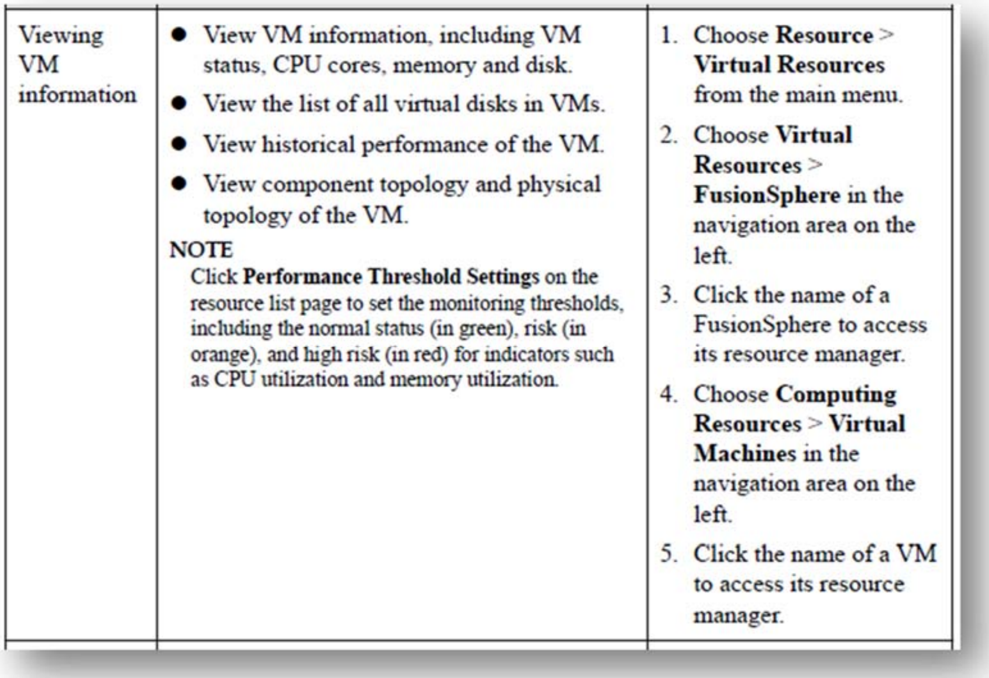
| '227 PATENT CLAIM 2 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | **Figure 5-3** Topology<br><br> <br>eSight Operations Guide Issue 08 (2018-08-28) at 213.<br>View the device status and its location on the network on the Current Alarms page. If the device color is red in the topology view, the alarm exists…. |

| '227 PATENT CLAIM 2 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |  <br>eSight Operations Guide Issue 08 (2018-08-28) at 235.<br>Further, virtual network nodes change color indicative of a vulnerability: |

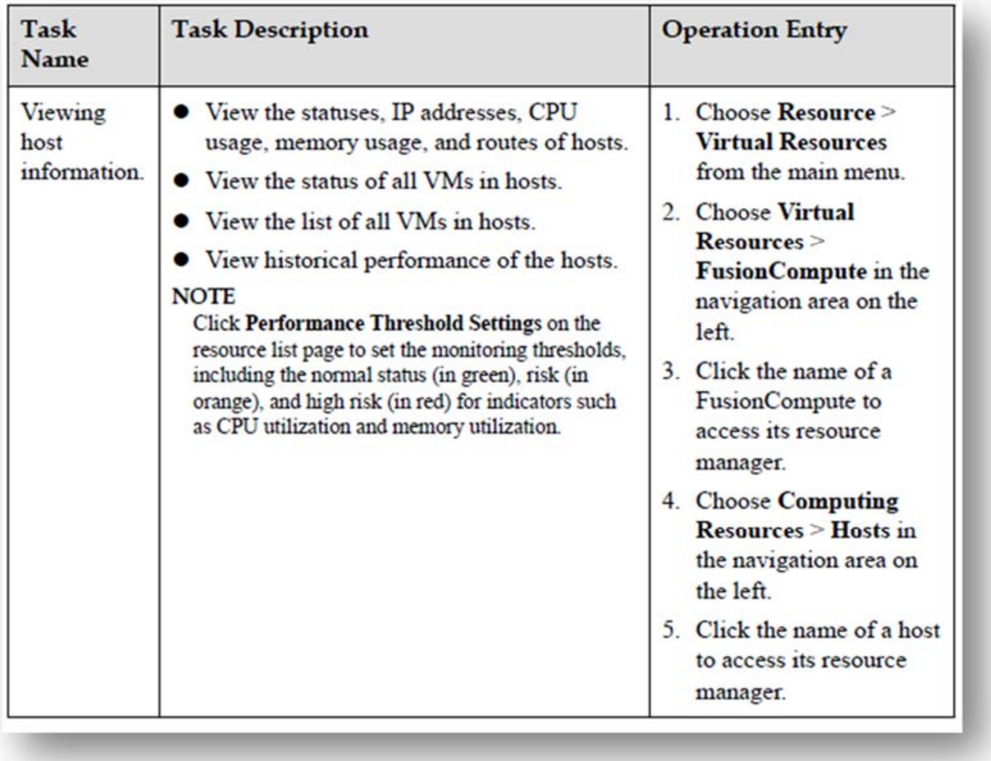
| '227 PATENT CLAIM 2 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | **Figure 11-4** VM component topology<br><br> Cloud Platform Layer<br>23<br>FC<br>FC_10.137.82.221<br>1<br>20.0%<br>23.4%<br>luxianchun--V3R5123<br>1<br>19.95%<br>23.37%<br>10.137.82.68<br>Virtualized Layer<br>1<br>VM<br>23.67KB/s<br>0.00KB/s<br>luxianchun--WINDOWS2...<br>23.67KB/s<br>0.0KB/s<br>i-0000017A-xvda<br>33.38KB/s<br>35.29KB/s<br>Network Adapter 0<br>2<br>Physical Layer<br>scsi-36234567890abcde...<br>4.07%<br>27.37%<br>PORT0<br>1<br>eSight Operations Guide Issue 08 (2018-08-28) at 944.<br>Additionally, virtual hosts and VMs have monitoring thresholds that result in network elements turning a different color indicative of a vulnerable network node (e.g., red for high risk, orange for risk, green for normal), as was further described above: |

| '227 PATENT CLAIM 2 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |  |

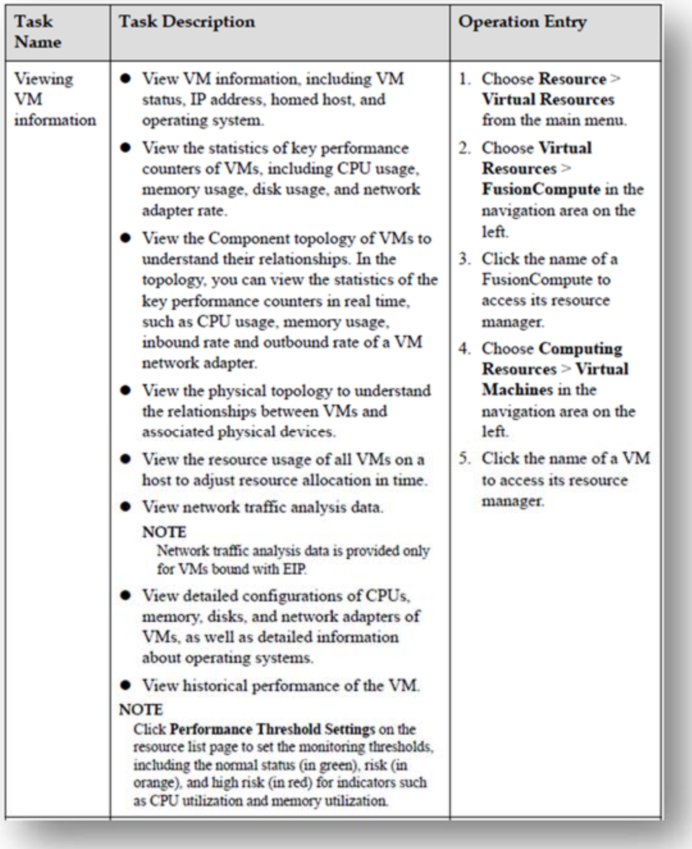
| | | |
|---|---|---|
| Viewing host information | ● View the running status, business IP addresses, and total CPU usage of hosts.<br>● View the list of all VMs in hosts.<br>● View historical performance of the hosts.<br>NOTE<br>Click **Performance Threshold Settings** on the resource list page to set the monitoring thresholds, including the normal status (in green), risk (in orange), and high risk (in red) for indicators such as CPU utilization and memory utilization. | 1. Choose **Resource** > **Virtual Resources** from the main menu.<br>2. Choose **Virtual Resources** > **FusionSphere** in the navigation area on the left.<br>3. Click the name of a FusionSphere to access its resource manager.<br>4. Choose **Computing Resources** > **Hosts** in the navigation area on the left.<br>5. Click the name of a host to access its resource manager. |

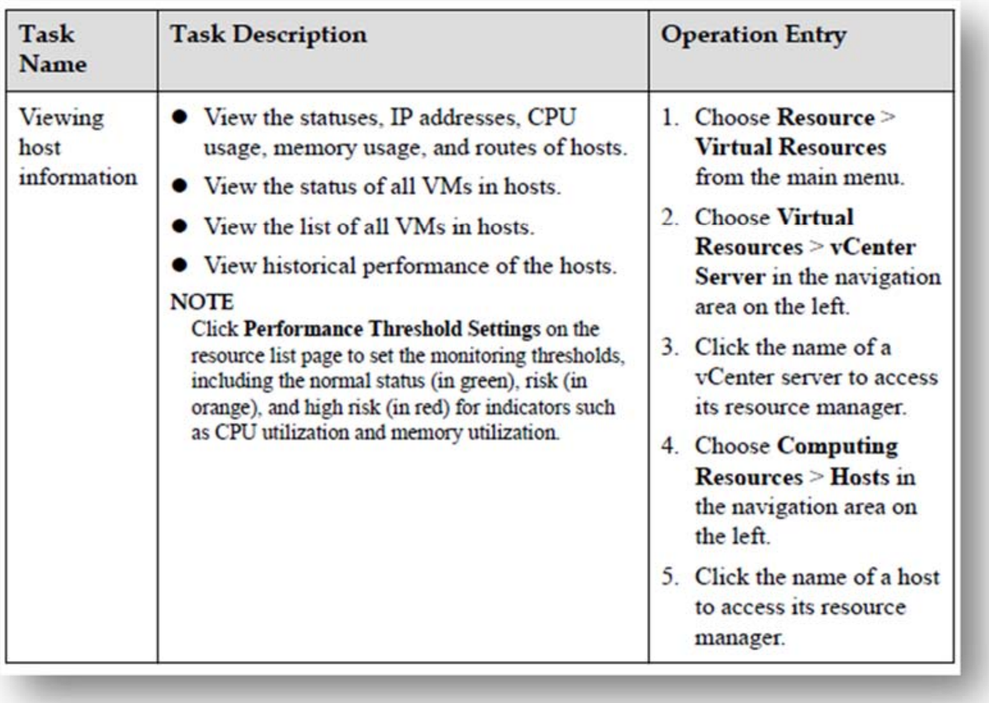
| '227 PATENT CLAIM 2 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
|  | <br>eSight Operations Guide Issue 08 (2018-08-28) at 966-67. |

| | | |
|---|---|---|
| Viewing VM information | ● View VM information, including VM status, CPU cores, memory and disk.<br>● View the list of all virtual disks in VMs.<br>● View historical performance of the VM.<br>● View component topology and physical topology of the VM.<br>NOTE<br>Click **Performance Threshold Settings** on the resource list page to set the monitoring thresholds, including the normal status (in green), risk (in orange), and high risk (in red) for indicators such as CPU utilization and memory utilization. | 1. Choose **Resource** > **Virtual Resources** from the main menu.<br>2. Choose **Virtual Resources** > **FusionSphere** in the navigation area on the left.<br>3. Click the name of a FusionSphere to access its resource manager.<br>4. Choose **Computing Resources** > **Virtual Machines** in the navigation area on the left.<br>5. Click the name of a VM to access its resource manager. |

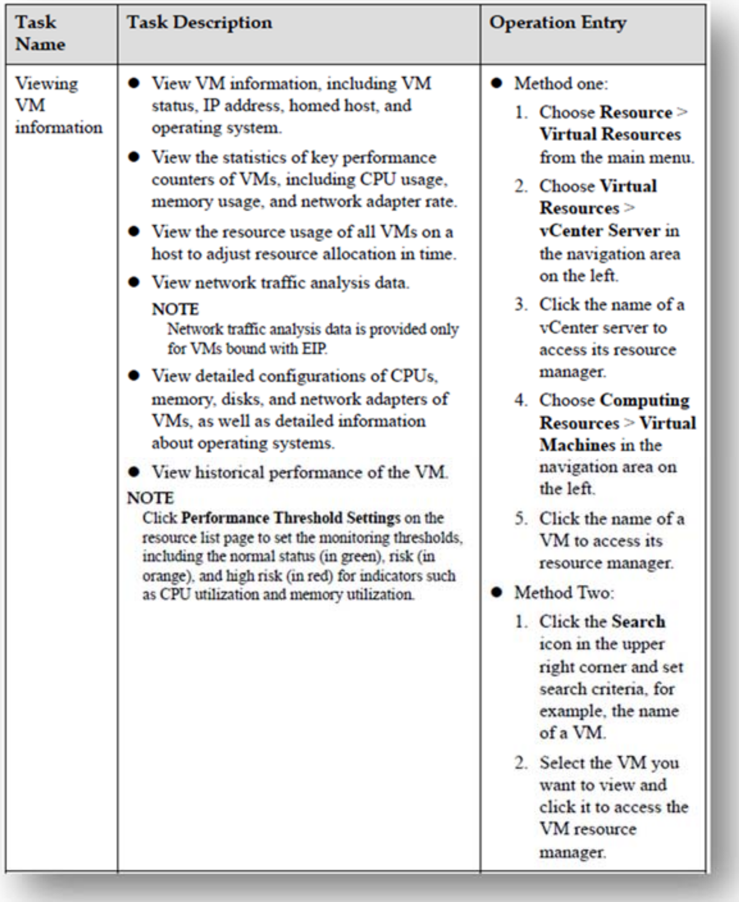
| '227 PATENT CLAIM 2 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
|  |  |

| Task Name | Task Description | Operation Entry |
|---|---|---|
| Viewing host information. | ● View the statuses, IP addresses, CPU usage, memory usage, and routes of hosts.<br>● View the status of all VMs in hosts.<br>● View the list of all VMs in hosts.<br>● View historical performance of the hosts.<br>NOTE<br>Click **Performance Threshold Settings** on the resource list page to set the monitoring thresholds, including the normal status (in green), risk (in orange), and high risk (in red) for indicators such as CPU utilization and memory utilization. | 1. Choose **Resource** > **Virtual Resources** from the main menu.<br>2. Choose **Virtual Resources** > **FusionCompute** in the navigation area on the left.<br>3. Click the name of a FusionCompute to access its resource manager.<br>4. Choose **Computing Resources** > **Hosts** in the navigation area on the left.<br>5. Click the name of a host to access its resource manager. |

<table>
<tr><th>'227 PATENT CLAIM 2</th><th>INFRINGEMENT BY HUAWEI CORPORATION</th></tr>
<tr><td></td><td>

<table>
<tr><th>Task Name</th><th>Task Description</th><th>Operation Entry</th></tr>
<tr><td>Viewing VM information</td><td>● View VM information, including VM status, IP address, homed host, and operating system.<br>● View the statistics of key performance counters of VMs, including CPU usage, memory usage, disk usage, and network adapter rate.<br>● View the Component topology of VMs to understand their relationships. In the topology, you can view the statistics of the key performance counters in real time, such as CPU usage, memory usage, inbound rate and outbound rate of a VM network adapter.<br>● View the physical topology to understand the relationships between VMs and associated physical devices.<br>● View the resource usage of all VMs on a host to adjust resource allocation in time.<br>● View network traffic analysis data.<br>NOTE<br>Network traffic analysis data is provided only for VMs bound with EIP.<br>● View detailed configurations of CPUs, memory, disks, and network adapters of VMs, as well as detailed information about operating systems.<br>● View historical performance of the VM.<br>NOTE<br>Click <b>Performance Threshold Settings</b> on the resource list page to set the monitoring thresholds, including the normal status (in green), risk (in orange), and high risk (in red) for indicators such as CPU utilization and memory utilization.</td><td>1. Choose <b>Resource</b> &gt; <b>Virtual Resources</b> from the main menu.<br>2. Choose <b>Virtual Resources</b> &gt; <b>FusionCompute</b> in the navigation area on the left.<br>3. Click the name of a FusionCompute to access its resource manager.<br>4. Choose <b>Computing Resources</b> &gt; <b>Virtual Machines</b> in the navigation area on the left.<br>5. Click the name of a VM to access its resource manager.</td></tr>
</table>
eSight Operations Guide Issue 08 (2018-08-28) at 982-83.
</td></tr>
</table>

| '227 PATENT CLAIM 2 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |  |

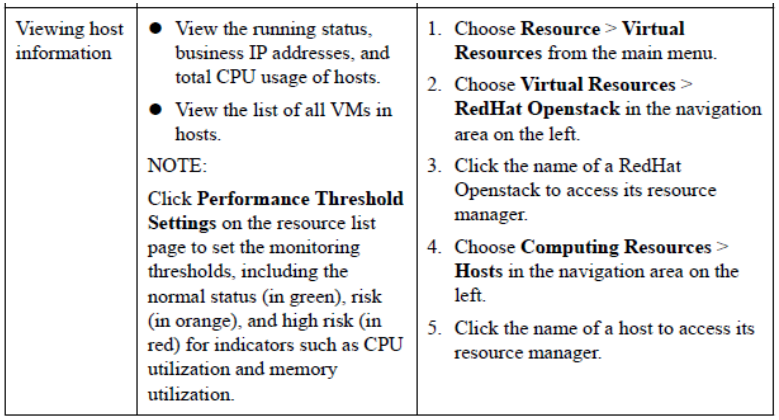
| Task Name | Task Description | Operation Entry |
|---|---|---|
| Viewing host information | ● View the statuses, IP addresses, CPU usage, memory usage, and routes of hosts.<br>● View the status of all VMs in hosts.<br>● View the list of all VMs in hosts.<br>● View historical performance of the hosts.<br>NOTE<br>Click **Performance Threshold Settings** on the resource list page to set the monitoring thresholds, including the normal status (in green), risk (in orange), and high risk (in red) for indicators such as CPU utilization and memory utilization. | 1. Choose **Resource** > **Virtual Resources** from the main menu.<br>2. Choose **Virtual Resources** > **vCenter Server** in the navigation area on the left.<br>3. Click the name of a vCenter server to access its resource manager.<br>4. Choose **Computing Resources** > **Hosts** in the navigation area on the left.<br>5. Click the name of a host to access its resource manager. |

| '227 PATENT CLAIM 2 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |  |

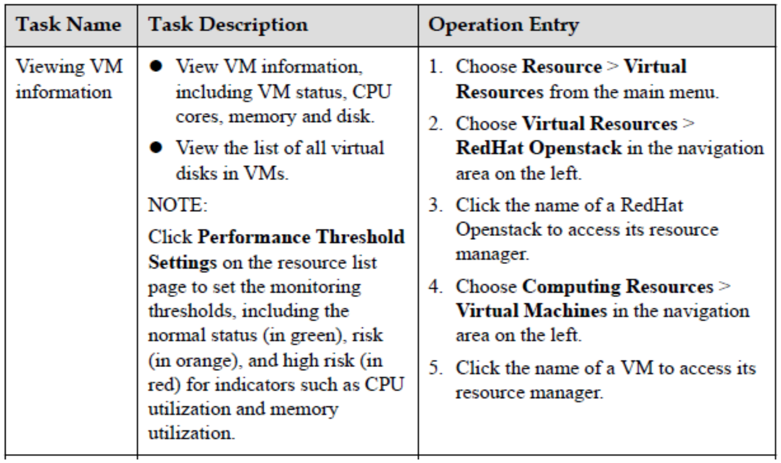
| Task Name | Task Description | Operation Entry |
|---|---|---|
| Viewing VM information | ● View VM information, including VM status, IP address, homed host, and operating system.<br>● View the statistics of key performance counters of VMs, including CPU usage, memory usage, and network adapter rate.<br>● View the resource usage of all VMs on a host to adjust resource allocation in time.<br>● View network traffic analysis data.<br>NOTE<br>Network traffic analysis data is provided only for VMs bound with EIP.<br>● View detailed configurations of CPUs, memory, disks, and network adapters of VMs, as well as detailed information about operating systems.<br>● View historical performance of the VM.<br>NOTE<br>Click **Performance Threshold Settings** on the resource list page to set the monitoring thresholds, including the normal status (in green), risk (in orange), and high risk (in red) for indicators such as CPU utilization and memory utilization. | ● Method one:<br>1. Choose **Resource** > **Virtual Resources** from the main menu.<br>2. Choose **Virtual Resources** > **vCenter Server** in the navigation area on the left.<br>3. Click the name of a vCenter server to access its resource manager.<br>4. Choose **Computing Resources** > **Virtual Machines** in the navigation area on the left.<br>5. Click the name of a VM to access its resource manager.<br>● Method Two:<br>1. Click the **Search** icon in the upper right corner and set search criteria, for example, the name of a VM.<br>2. Select the VM you want to view and click it to access the VM resource manager. |

eSight Operations Guide Issue 08 (2018-08-28) at 997-998.

| '227 PATENT CLAIM 2 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|



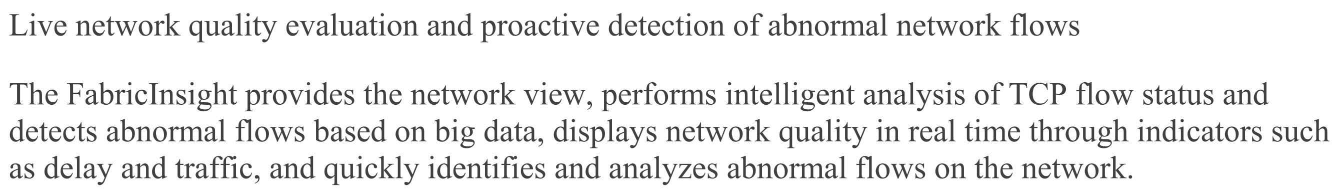
| | | |
|---|---|---|
| Viewing host information | ● View the running status, business IP addresses, and total CPU usage of hosts.<br>● View the list of all VMs in hosts.<br>NOTE:<br>Click **Performance Threshold Settings** on the resource list page to set the monitoring thresholds, including the normal status (in green), risk (in orange), and high risk (in red) for indicators such as CPU utilization and memory utilization. | 1. Choose **Resource** > **Virtual Resources** from the main menu.<br>2. Choose **Virtual Resources** > **RedHat Openstack** in the navigation area on the left.<br>3. Click the name of a RedHat Openstack to access its resource manager.<br>4. Choose **Computing Resources** > **Hosts** in the navigation area on the left.<br>5. Click the name of a host to access its resource manager. |

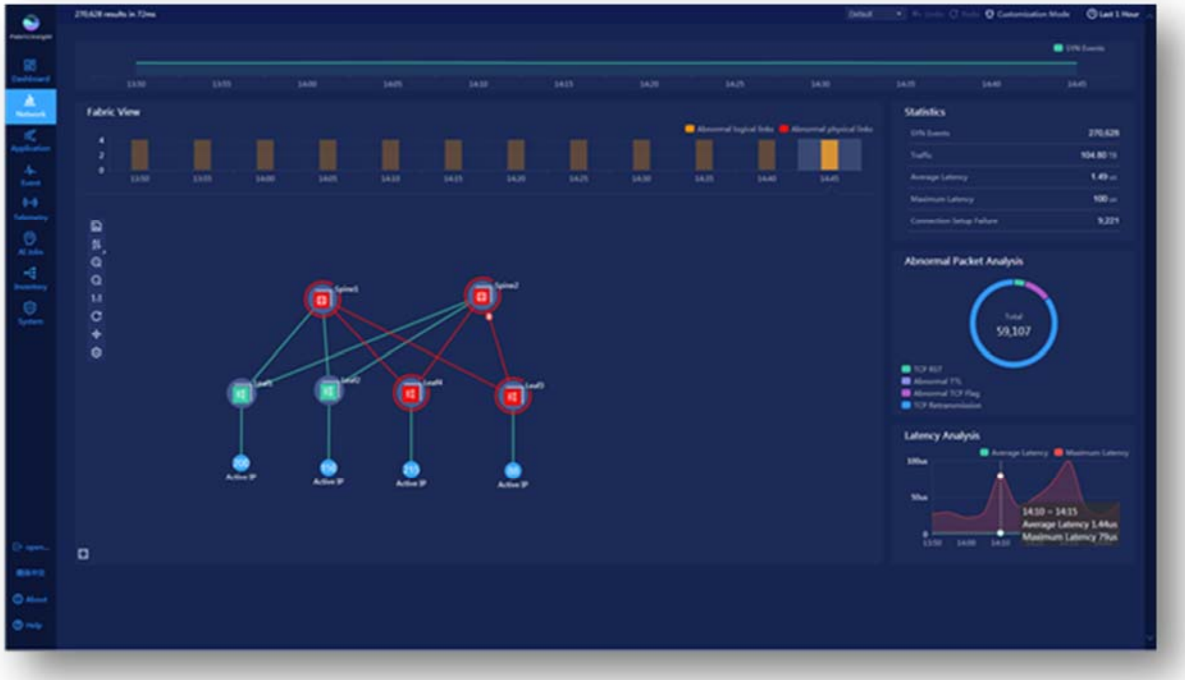


| Task Name | Task Description | Operation Entry |
|---|---|---|
| Viewing VM information | ● View VM information, including VM status, CPU cores, memory and disk.<br>● View the list of all virtual disks in VMs.<br>NOTE:<br>Click **Performance Threshold Settings** on the resource list page to set the monitoring thresholds, including the normal status (in green), risk (in orange), and high risk (in red) for indicators such as CPU utilization and memory utilization. | 1. Choose **Resource** > **Virtual Resources** from the main menu.<br>2. Choose **Virtual Resources** > **RedHat Openstack** in the navigation area on the left.<br>3. Click the name of a RedHat Openstack to access its resource manager.<br>4. Choose **Computing Resources** > **Virtual Machines** in the navigation area on the left.<br>5. Click the name of a VM to access its resource manager. |

eSight Operations Guide Issue 08 (2018-08-28) at 1014-15.

Further, in FabricInsights network elements turn a different color indicative of a vulnerable network node. For example:

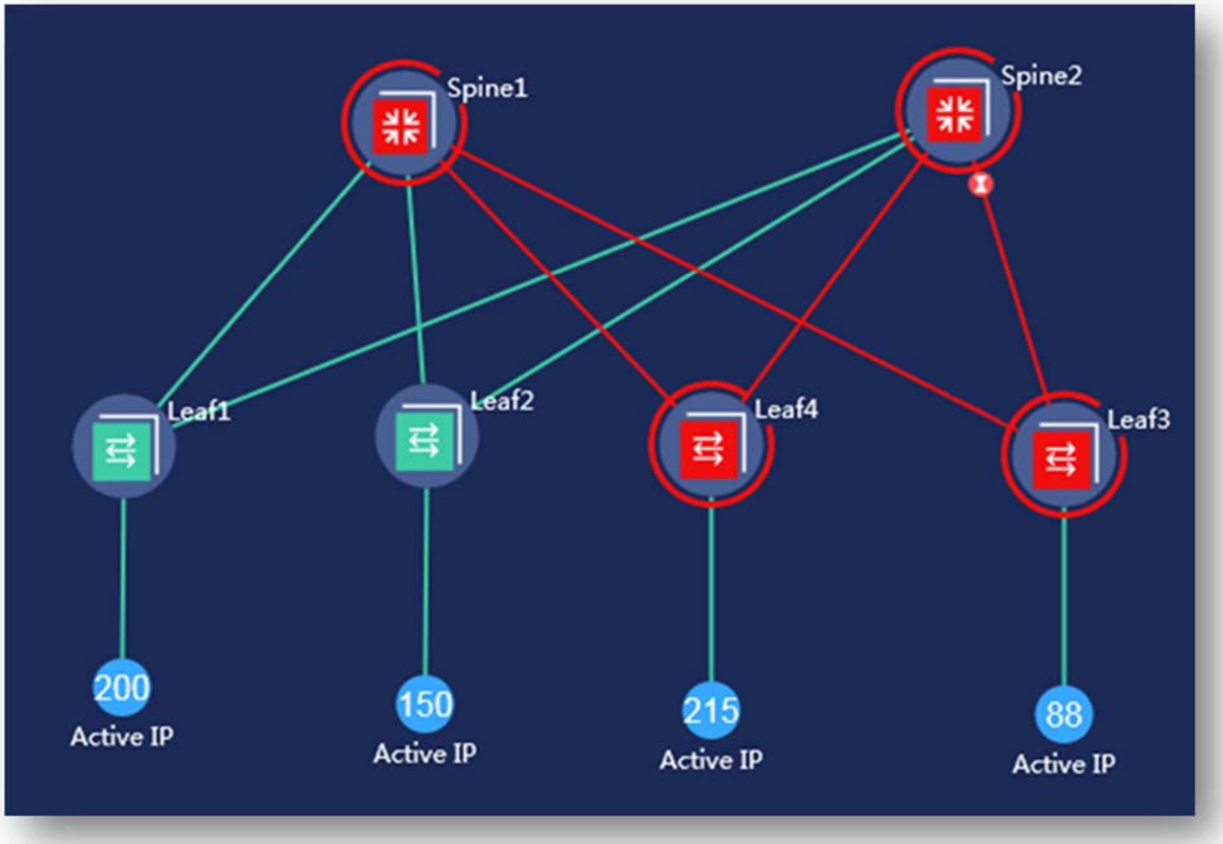
| '227 PATENT CLAIM 2 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |  Live network quality evaluation and proactive detection of abnormal network flows<br>The FabricInsight provides the network view, performs intelligent analysis of TCP flow status and detects abnormal flows based on big data, displays network quality in real time through indicators such as delay and traffic, and quickly identifies and analyzes abnormal flows on the network. |

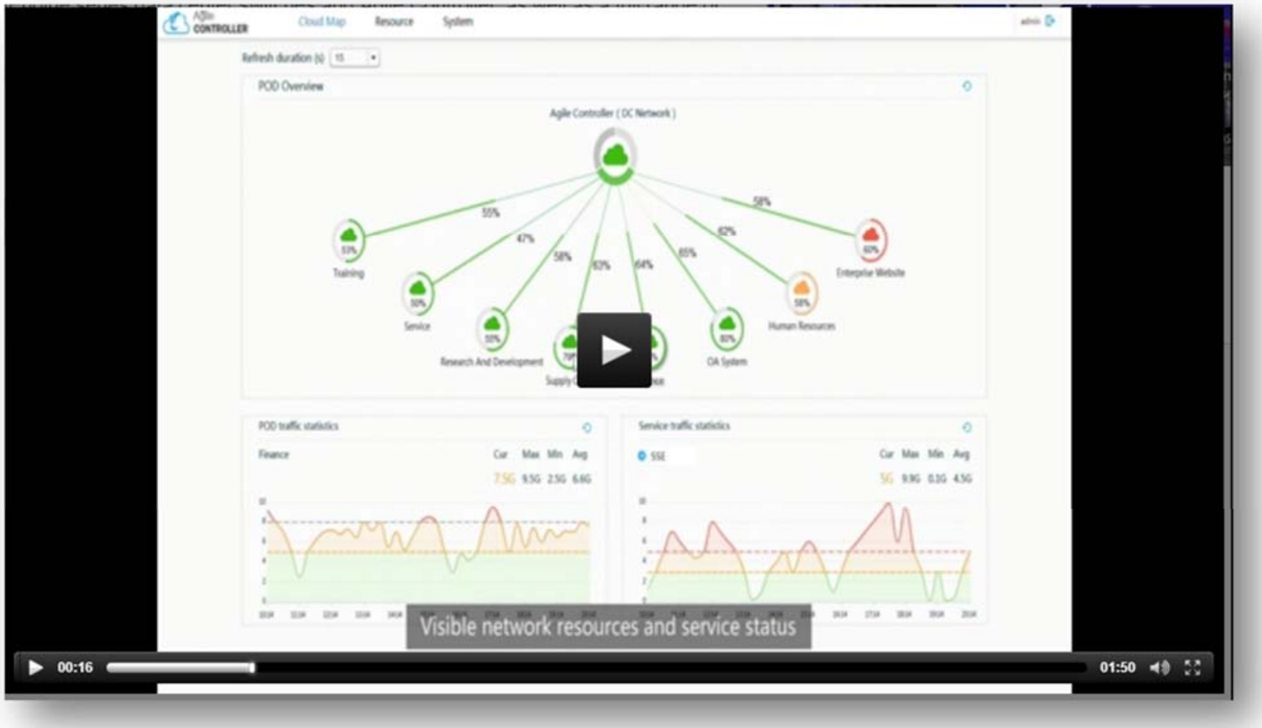
| '227 PATENT CLAIM 2 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |  |

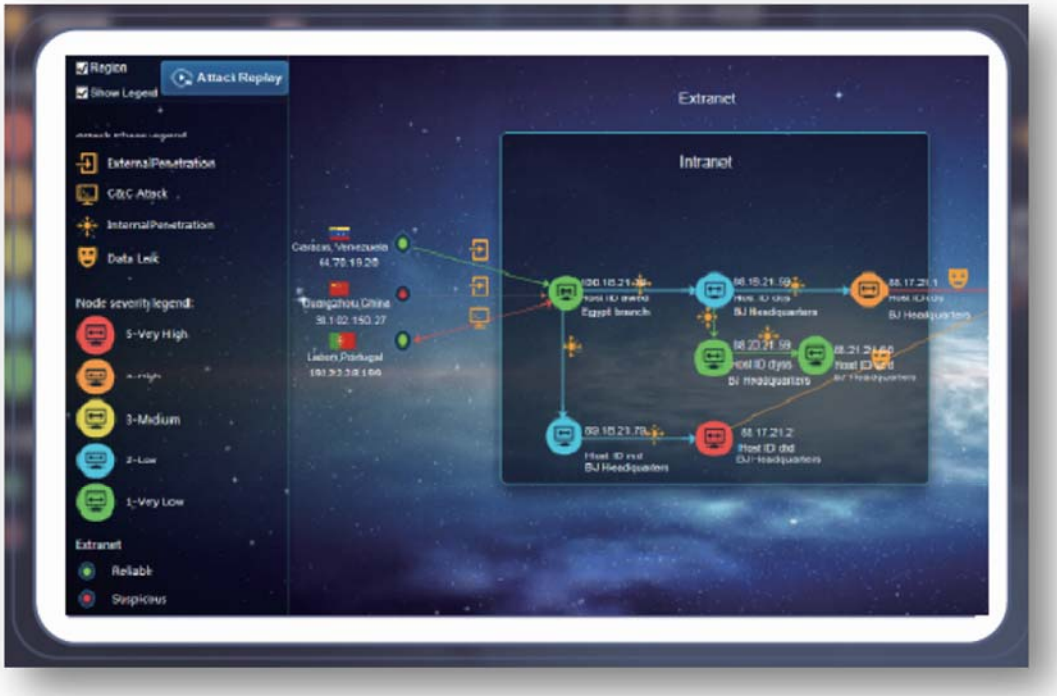
Statistics

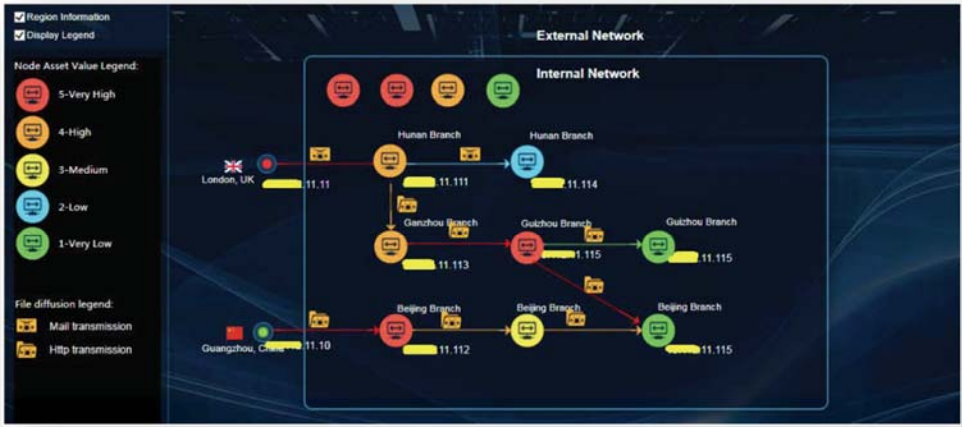
| | |
|---|---|
| SYN Events | 270,628 |
| Traffic | 104.80 TB |
| Average Latency | 1.49 us |
| Maximum Latency | 100 us |
| Connection Setup Failure | 9,221 |

14:10 – 14:15
Average Latency 1.44us
Maximum Latency 79us

| '227 PATENT CLAIM 2 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |  Spine1<br>Spine2<br>Leaf1<br>Leaf2<br>Leaf4<br>Leaf3<br>200<br>Active IP<br>150<br>Active IP<br>215<br>Active IP<br>88<br>Active IP<br>Huawei FabricInsight Datasheet at 3-4.<br>In the Agile Controller, network elements turn a different color indicative of a vulnerable network node: |

| '227 PATENT CLAIM 2 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |   Agile CONTROLLER<br>Cloud Map<br>Resource<br>System<br>admin<br>Refresh duration (s) 15<br>POD Overview<br>Agile Controller ( DC Network )<br>55%<br>47%<br>58%<br>63%<br>64%<br>65%<br>62%<br>58%<br>Training<br>Service<br>Research And Development<br>Supply<br>OA System<br>Human Resources<br>Enterprise Website<br>POD traffic statistics<br>Finance<br>Cur Max Min Avg<br>Service traffic statistics<br>SSE<br>Visible network resources and service status<br>00:16<br>01:50<br>Huawei Video: *Cloud Fabric: Huawei and VMWare Innovate* (e.huawei.com/en-US/videos/global/older/hw_362493) (Huawei and VMWare co-operate on an SDN data center networking solution) at 0:16.<br><br>In the CIS, network elements turn a different color indicative of a vulnerable network node: |

| '227 PATENT CLAIM 2 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | <br> ☑ Region<br>☑ Show Legend<br>Attack Replay<br>Extranet<br>Intranet<br>ExternalPenetration<br>C&C Attack<br>InternalPenetration<br>Data Leak<br>Node severity legend:<br>5-Very High<br>4-High<br>3-Medium<br>2-Low<br>1-Very Low<br>Extranet<br>Reliable<br>Suspicious<br>Caracas, Venezuela<br>44.78.19.28<br>Guangzhou China<br>98.1.02.150.27<br>Lisbon Portugal<br>100.18.21.<br>Egypt branch<br>88.18.21.59<br>BJ Headquarters<br>88.17.21.1<br>BJ Headquarters<br>88.20.21.59<br>Host ID dyss<br>BJ Headquarters<br>88.21.21.60<br>Host ID<br>BJ Headquarters<br>89.18.21.78<br>Host ID<br>BJ Headquarters<br>88.17.21.2<br>Host ID dkd<br>BJ Headquarters<br>The CIS visually displays multiple attack stages of advanced threats and asset information of key Nodes…<br>Huawei CIS Cybersecurity Intelligence System Product Description at 3. |

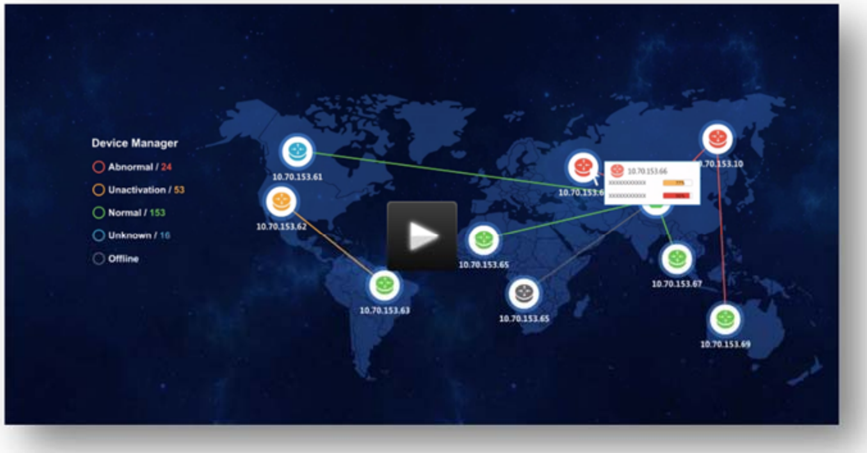
| '227 PATENT CLAIM 2 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
|  | *See also, e.g.,:*<br><br>☑ Region Information<br>☑ Display Legend<br> External Network<br>Internal Network<br>Node Asset Value Legend:<br>5-Very High<br>4-High<br>3-Medium<br>2-Low<br>1-Very Low<br>File diffusion legend:<br>Mail transmission<br>Http transmission<br>London, UK<br>11.11<br>Hunan Branch<br>11.111<br>Hunan Branch<br>11.114<br>Ganzhou Branch<br>11.113<br>Guizhou Branch<br>1.115<br>Guizhou Branch<br>11.115<br>Guangzhou, China<br>11.10<br>Beijing Branch<br>11.112<br>Beijing Branch<br>Beijing Branch<br>11.115<br>Huawei CIS Cybersecurity Intelligence System Datasheet at 4. |

| '227 PATENT CLAIM 3 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| **3.** A graphical user interface according to claim 1, and further comprising a manager window for | The Huawei '227 Patent Accused Instrumentalities infringe this claim. *See* Claim 1.<br>The Accused Instrumentalities further comprise a manager window for displaying properties of network elements. |

<table>
<tr><th>'227 PATENT<br>CLAIM 3</th><th>INFRINGEMENT BY HUAWEI CORPORATION</th></tr>
<tr><td>displaying properties of network elements.</td><td>

For example, eSight allows users to view a manager window for displaying properties of network elements.

> "Clicking on a device in the topology view allows you to learn about its running status and alarms."



Unified View video at 0:30 https://e.huawei.com/en/products/software/mgmt-sys/esight/esight-platform

Though the GUI is not shown in the eSight documentation in conjunction with each explanation below, on information and belief, there is a corresponding GUI with a manager window that displays properties of network elements:

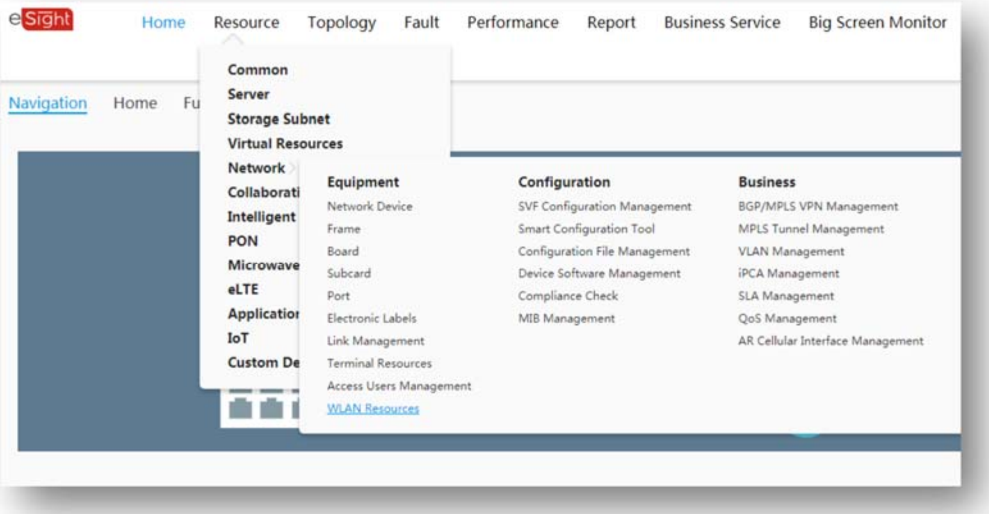
> 11.3.6 Abnormal Communication of VMs

</td></tr>
</table>

| '227 Patent Claim 3 | Infringement By Huawei Corporation |
|---|---|
|  | When a service exception occurs, for example, network disconnection or data transmission discontinuity, you can locate fault causes using the detailed data on the VM resource management page.<br>…<br>Procedure<br>Step 1 Click the Search icon in the upper right corner and set search criteria, for example, the name of a VM.<br>Step 2 Select the VM you want to view and click it to access its resource manager.<br>Step 3 Choose General > Basic Information in the navigation area on the left. Then check and handle static configuration information of the VM.<br>Step 4 Choose General > Alarm List in the navigation area on the left. Then check and handle alarms related to the fault.<br>Step 5 Choose General > Physical Topology in the navigation area on the left. Then check and handle VM network connection problems.<br>Step 6 Choose Details > Component Topology in the navigation area on the left. Then check and handle VM performance statistics.<br>Click in the upper left corner to modify performance counters you want to display in the topology.<br>If the statistics of key performance counters such as memory usage, CPU usage, and disk read/write rate of the VM are incorrect, services running on the VM consumes excess |

| ’227 PATENT CLAIM 3 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | CPU and memory resources. In this case, adjust services or expand the capacity of the VM.<br>----End<br>eSight Operations Guide Issue 08 (2018-08-28) at 973.<br>Checking Service Information<br>In the service list or topology, you can view the alarms, topologies, tunnels, service configurations, real-time performance, and global parameters of IPSec VPN services.<br>…<br>– In the topology, right-click a device to monitor device information.<br>- Select View Alarms to view alarm information on the device.<br>- Select Device Manage to go to the device resource management page and manage the device.<br>- Select Monitor Realtime Performance to go to the Realtime Performance page, select Performance counter, Resource, and Collection period, and view the global IPSec performance data of this device.<br>eSight Operations Guide Issue 08 (2018-08-28) at 1659-61.<br>12.11.5.4 Viewing Regional Detailed Information |

*Harris Corporation v. Huawei, et al* – **Case No. 2:18-cv-439**
**Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)**
**Exhibit A – U.S. Patent No. 6,535,227 ('227) – Claims 1-6, 8-13, 15-20, 22, 24**

| '227 PATENT<br>CLAIM 3 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
|  | eSight allows users to view resource details including the AC, AP, user, and SSID information in each region in real time.<br>Prerequisites<br>Enter the Region Object Manager.<br>Choose Resource > Network > Equipment > WLAN Resources from the main menu.<br><br> eSight<br>Home<br>Resource<br>Topology<br>Fault<br>Performance<br>Report<br>Business Service<br>Big Screen Monitor<br>Navigation<br>Home<br>Fu<br>Common<br>Server<br>Storage Subnet<br>Virtual Resources<br>Network<br>Collaborati<br>Intelligent<br>PON<br>Microwave<br>eLTE<br>Applicatior<br>IoT<br>Custom De<br>Equipment<br>Network Device<br>Frame<br>Board<br>Subcard<br>Port<br>Electronic Labels<br>Link Management<br>Terminal Resources<br>Access Users Management<br>WLAN Resources<br>Configuration<br>SVF Configuration Management<br>Smart Configuration Tool<br>Configuration File Management<br>Device Software Management<br>Compliance Check<br>MIB Management<br>Business<br>BGP/MPLS VPN Management<br>MPLS Tunnel Management<br>VLAN Management<br>iPCA Management<br>SLA Management<br>QoS Management<br>AR Cellular Interface Management |

| '227 PATENT CLAIM 3 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|

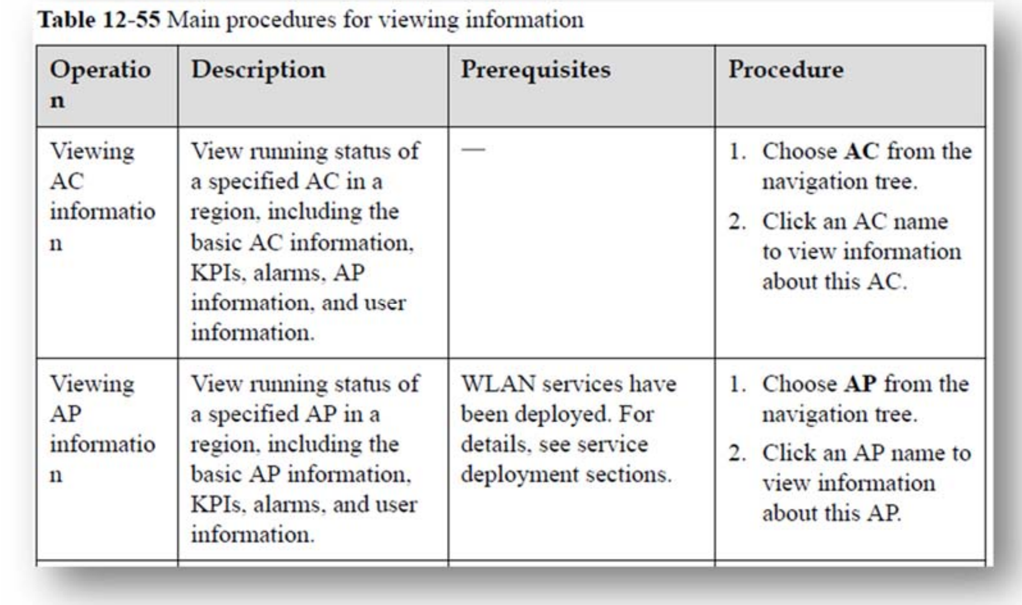


**Table 12-55** Main procedures for viewing information

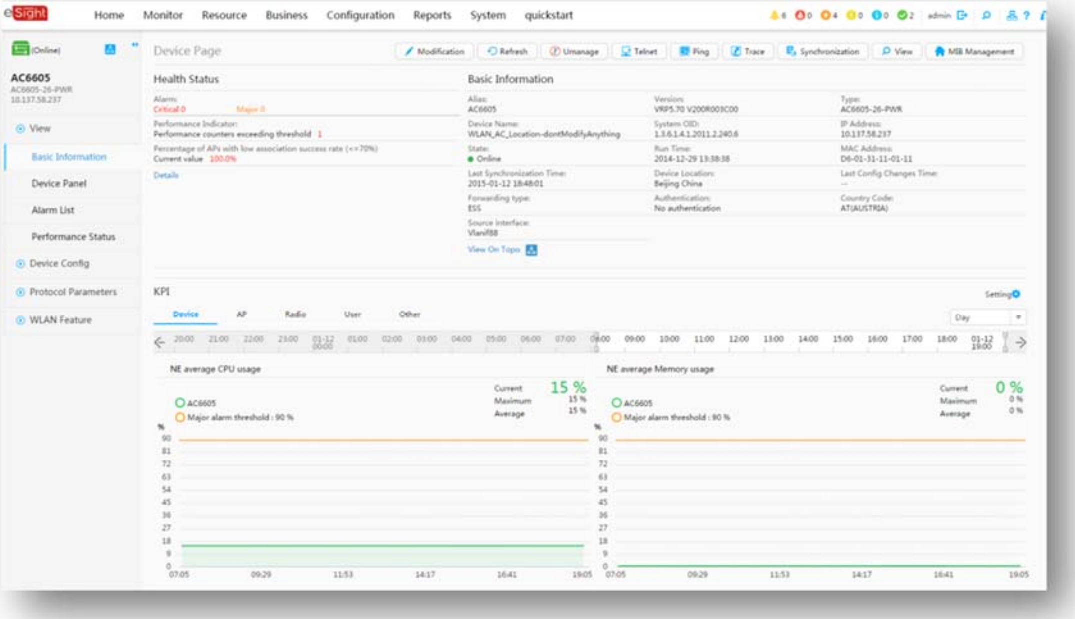
| Operation | Description | Prerequisites | Procedure |
|---|---|---|---|
| Viewing AC information | View running status of a specified AC in a region, including the basic AC information, KPIs, alarms, AP information, and user information. | — | 1. Choose **AC** from the navigation tree.<br>2. Click an AC name to view information about this AC. |
| Viewing AP information | View running status of a specified AP in a region, including the basic AP information, KPIs, alarms, and user information. | WLAN services have been deployed. For details, see service deployment sections. | 1. Choose **AP** from the navigation tree.<br>2. Click an AP name to view information about this AP. |

…

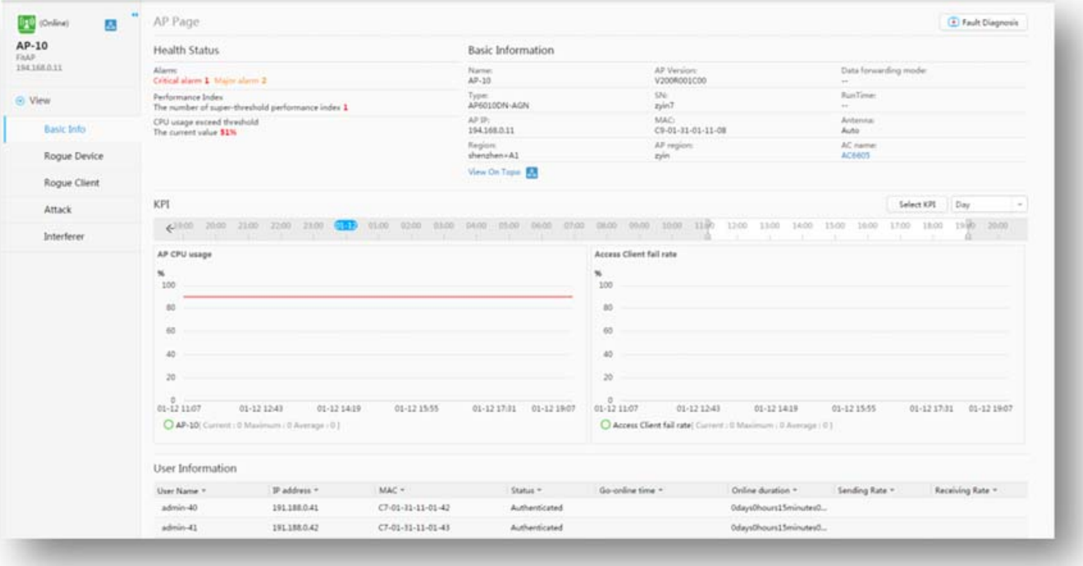
eSight Operations Guide Issue 08 (2018-08-28) at 1363-64.

*See also*, eSight WLAN White Paper explaining "Users can view statistics about ACs, fit APs, SSIDs, STAs, and unauthorized APs in resource management and view wireless resource topologies in WLAN service topology views and location topology views in the AC/AP network and region deployment dimensions." And showing exemplary AC Object Manager:

*Harris Corporation v. Huawei, et al* – **Case No. 2:18-cv-439**
**Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)**
**Exhibit A – U.S. Patent No. 6,535,227 ('227) – Claims 1-6, 8-13, 15-20, 22, 24**

| '227 PATENT CLAIM 3 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | <br> eSight<br>Home<br>Monitor<br>Resource<br>Business<br>Configuration<br>Reports<br>System<br>quickstart<br>admin<br>(Online)<br>View<br>Basic Information<br>Device Panel<br>Alarm List<br>Performance Status<br>Device Config<br>Protocol Parameters<br>WLAN Feature<br>Modification<br>Refresh<br>Umanage<br>Telnet<br>Ping<br>Trace<br>Synchronization<br>View<br>MIB Management<br>Details<br>View On Topo<br>Setting<br>Day<br>Device<br>AP<br>Radio<br>User<br>Other<br>AC6605<br>AC6605-26-PWR<br>10.137.58.237<br>Device Page<br>Health Status<br>Alarm:<br>Critical 0 Major 0<br>Performance Indicator:<br>Performance counters exceeding threshold 1<br>Percentage of APs with low association success rate (<=70%)<br>Current value 100.0%<br>Basic Information<br>Alias: AC6605<br>Version: VRP5.70 V200R003C00<br>Type: AC6605-26-PWR<br>Device Name: WLAN_AC_Location-dontModifyAnything<br>System OID: 1.3.6.1.4.1.2011.2.240.6<br>IP Address: 10.137.58.237<br>State: ● Online<br>Run Time: 2014-12-29 13:38:38<br>MAC Address: D6-01-31-11-01-11<br>Last Synchronization Time: 2015-01-12 18:48:01<br>Device Location: Beijing China<br>Last Config Changes Time: --<br>Forwarding type: ESS<br>Authentication: No authentication<br>Country Code: AT(AUSTRIA)<br>Source interface: Vlanif88<br>KPI<br>NE average CPU usage<br>AC6605<br>Major alarm threshold : 90 %<br>Current 15 %<br>Maximum 15 %<br>Average 15 %<br>NE average Memory usage<br>AC6605<br>Major alarm threshold : 90 %<br>Current 0 %<br>Maximum 0 %<br>Average 0 %<br><br>HUAWEI eSight WLAN White Paper Issue 01 (2017-03-20) at 26.<br><br>And exemplary AP Object Manager: |

| '227 PATENT CLAIM 3 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | |



Health Status

Alarm:
Critical alarm 1 Major alarm 2

Performance Index
The number of super-threshold performance index 1

CPU usage exceed threshold
The current value 91%

Basic Information

| | | |
|---|---|---|
| Name:<br>AP-10 | AP Version:<br>V200R001C00 | Data forwarding mode:<br>-- |
| Type:<br>AP6010DN-AGN | SN:<br>zyin7 | RunTime:<br>-- |
| AP IP:<br>194.168.0.11 | MAC:<br>C9-01-31-01-11-08 | Antenna:<br>Auto |
| Region:<br>shenzhen+A1 | AP region:<br>zyin | AC name:<br>AC6605 |

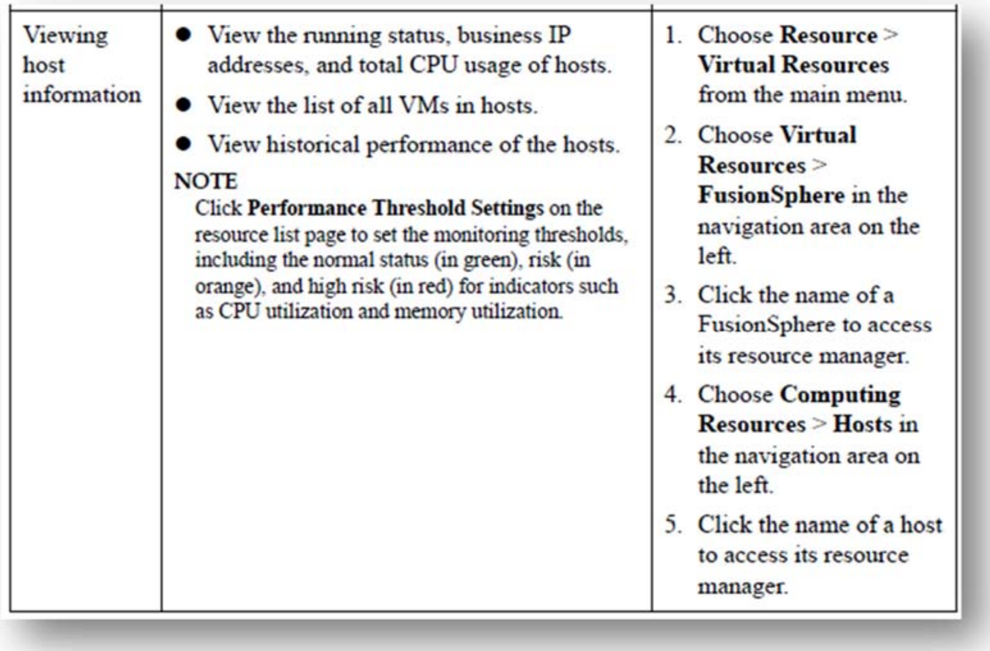
View On Topo

User Information

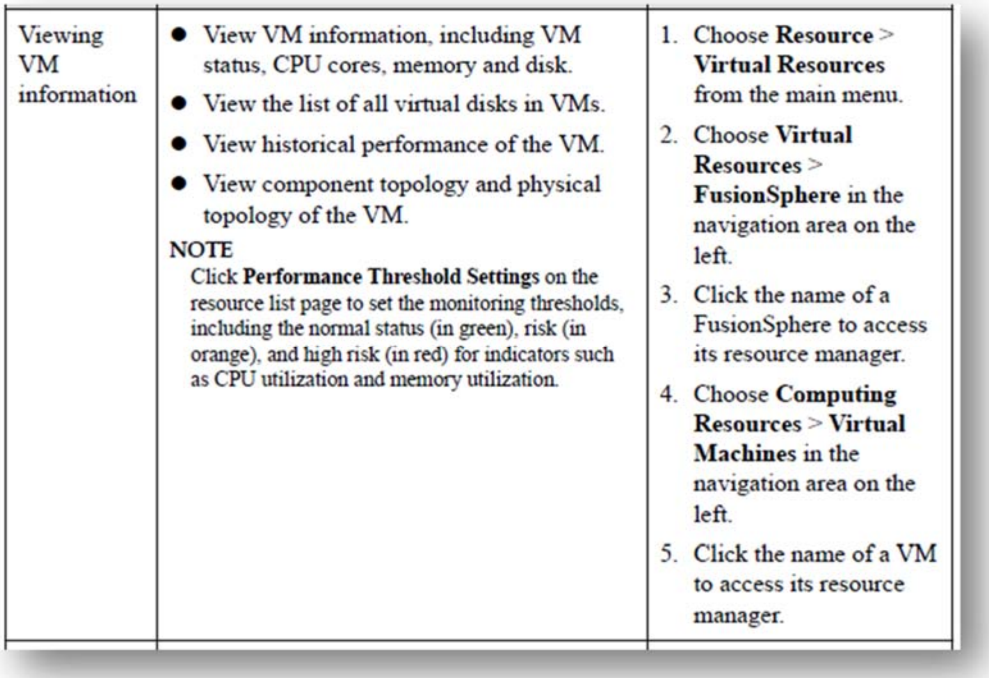
| User Name | IP address | MAC | Status | Go-online time | Online duration | Sending Rate | Receiving Rate |
|---|---|---|---|---|---|---|---|
| admin-40 | 191.188.0.41 | C7-01-31-11-01-42 | Authenticated | | 0days0hours15minutes0... | | |
| admin-41 | 191.188.0.42 | C7-01-31-11-01-43 | Authenticated | | 0days0hours15minutes0... | | |

HUAWEI eSight WLAN White Paper Issue 01 (2017-03-20) at 27.

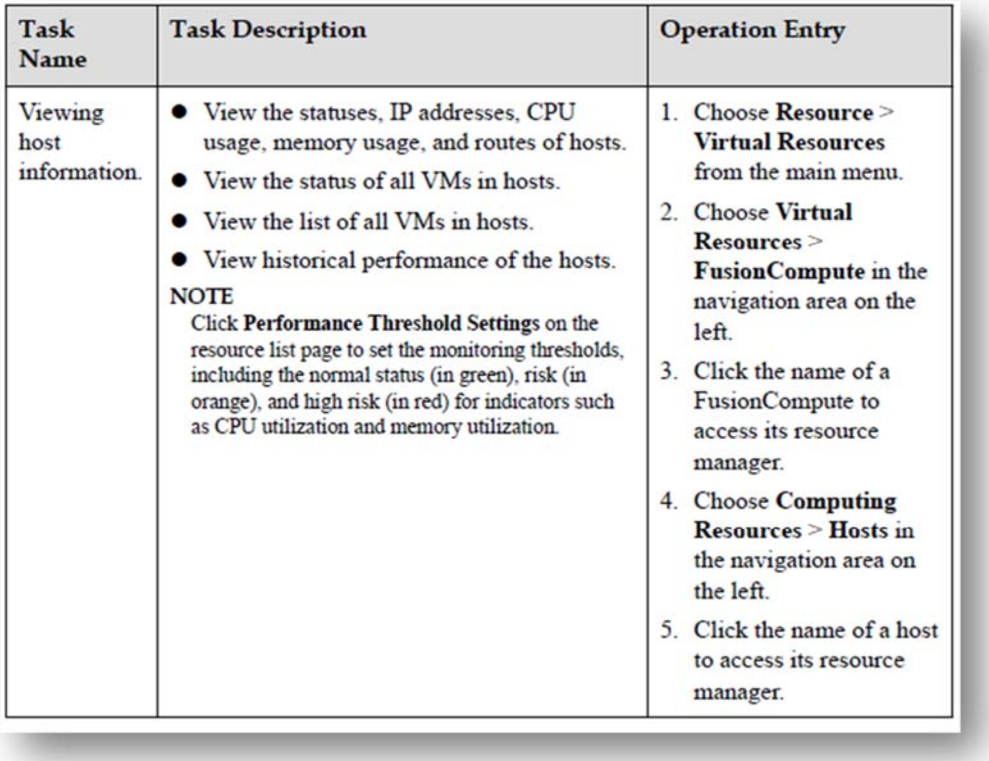
In a virtual environment a manager window displays properties of host and/or VM network elements, as described below, for example:

| '227 PATENT CLAIM 3 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |  |

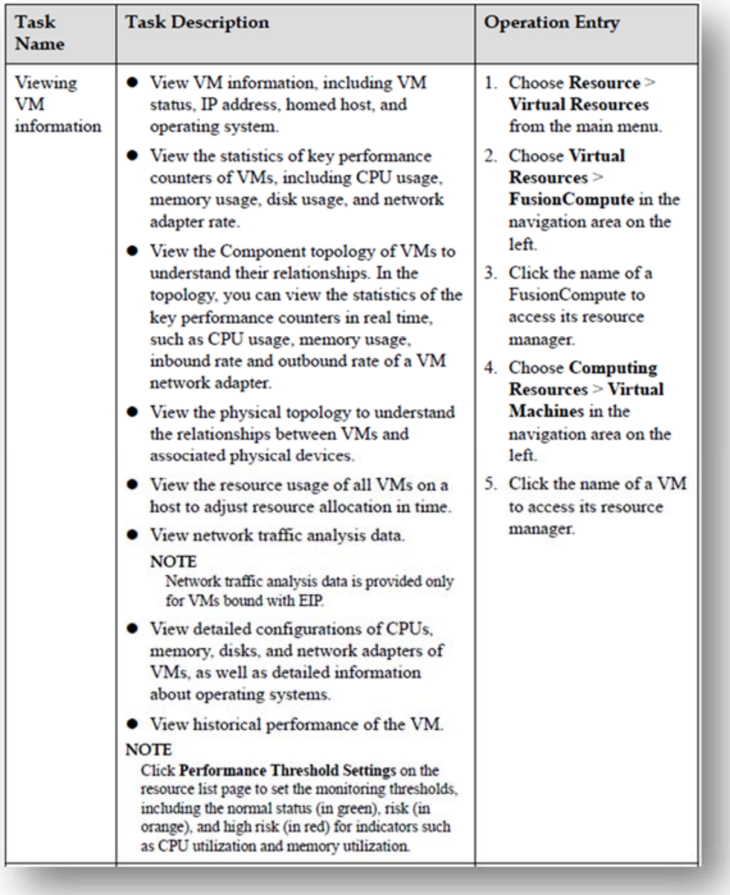
| | | |
|---|---|---|
| Viewing host information | ● View the running status, business IP addresses, and total CPU usage of hosts.<br>● View the list of all VMs in hosts.<br>● View historical performance of the hosts.<br>NOTE<br>Click **Performance Threshold Settings** on the resource list page to set the monitoring thresholds, including the normal status (in green), risk (in orange), and high risk (in red) for indicators such as CPU utilization and memory utilization. | 1. Choose **Resource** > **Virtual Resources** from the main menu.<br>2. Choose **Virtual Resources** > **FusionSphere** in the navigation area on the left.<br>3. Click the name of a FusionSphere to access its resource manager.<br>4. Choose **Computing Resources** > **Hosts** in the navigation area on the left.<br>5. Click the name of a host to access its resource manager. |

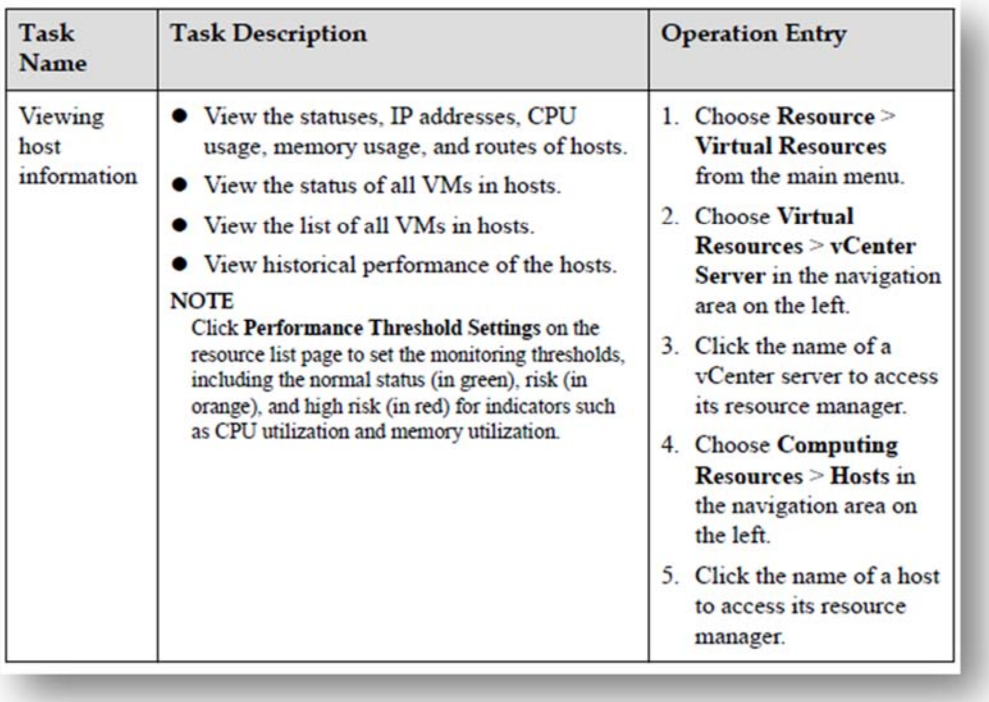
<table>
<tr><th>'227 PATENT CLAIM 3</th><th>INFRINGEMENT BY HUAWEI CORPORATION</th></tr>
<tr><td></td><td>

<table>
<tr><td>Viewing VM information</td><td>● View VM information, including VM status, CPU cores, memory and disk.<br>● View the list of all virtual disks in VMs.<br>● View historical performance of the VM.<br>● View component topology and physical topology of the VM.<br>NOTE<br>Click <b>Performance Threshold Settings</b> on the resource list page to set the monitoring thresholds, including the normal status (in green), risk (in orange), and high risk (in red) for indicators such as CPU utilization and memory utilization.</td><td>1. Choose <b>Resource</b> &gt; <b>Virtual Resources</b> from the main menu.<br>2. Choose <b>Virtual Resources</b> &gt; <b>FusionSphere</b> in the navigation area on the left.<br>3. Click the name of a FusionSphere to access its resource manager.<br>4. Choose <b>Computing Resources</b> &gt; <b>Virtual Machines</b> in the navigation area on the left.<br>5. Click the name of a VM to access its resource manager.</td></tr>
</table>
eSight Operations Guide Issue 08 (2018-08-28) at 966-67.
</td></tr>
</table>

*Harris Corporation v. Huawei, et al* – **Case No. 2:18-cv-439**
**Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)**
**Exhibit A – U.S. Patent No. 6,535,227 ('227) – Claims 1-6, 8-13, 15-20, 22, 24**

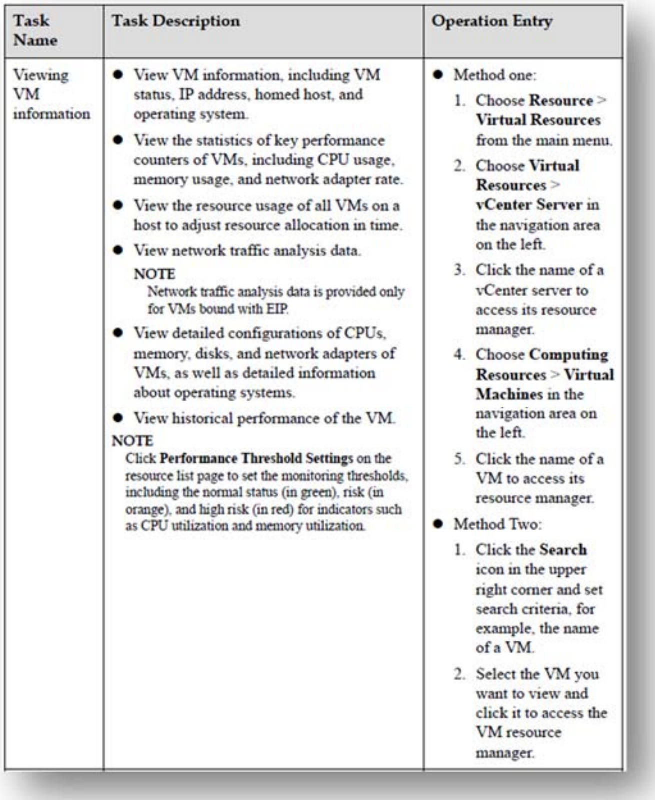
| **'227 PATENT CLAIM 3** | **INFRINGEMENT BY HUAWEI CORPORATION** |
|---|---|
|  |  |

| Task Name | Task Description | Operation Entry |
|---|---|---|
| Viewing host information. | ● View the statuses, IP addresses, CPU usage, memory usage, and routes of hosts.<br>● View the status of all VMs in hosts.<br>● View the list of all VMs in hosts.<br>● View historical performance of the hosts.<br>NOTE<br>Click **Performance Threshold Settings** on the resource list page to set the monitoring thresholds, including the normal status (in green), risk (in orange), and high risk (in red) for indicators such as CPU utilization and memory utilization. | 1. Choose **Resource** > **Virtual Resources** from the main menu.<br>2. Choose **Virtual Resources** > **FusionCompute** in the navigation area on the left.<br>3. Click the name of a FusionCompute to access its resource manager.<br>4. Choose **Computing Resources** > **Hosts** in the navigation area on the left.<br>5. Click the name of a host to access its resource manager. |

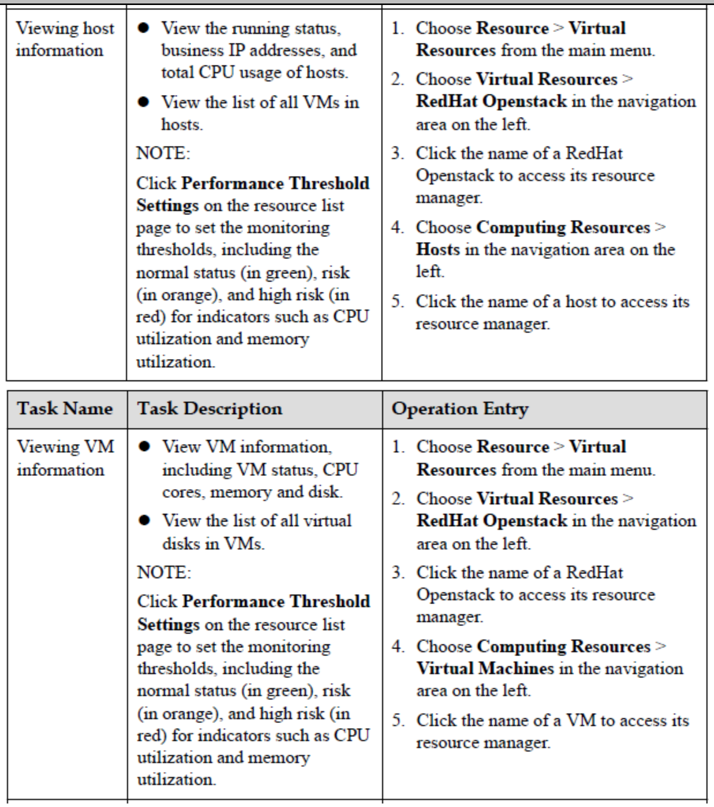
<table>
<tr><th>'227 PATENT CLAIM 3</th><th>INFRINGEMENT BY HUAWEI CORPORATION</th></tr>
<tr><td></td><td>

<table>
<tr><th>Task Name</th><th>Task Description</th><th>Operation Entry</th></tr>
<tr><td>Viewing VM information</td><td>● View VM information, including VM status, IP address, homed host, and operating system.<br>● View the statistics of key performance counters of VMs, including CPU usage, memory usage, disk usage, and network adapter rate.<br>● View the Component topology of VMs to understand their relationships. In the topology, you can view the statistics of the key performance counters in real time, such as CPU usage, memory usage, inbound rate and outbound rate of a VM network adapter.<br>● View the physical topology to understand the relationships between VMs and associated physical devices.<br>● View the resource usage of all VMs on a host to adjust resource allocation in time.<br>● View network traffic analysis data.<br>NOTE<br>Network traffic analysis data is provided only for VMs bound with EIP.<br>● View detailed configurations of CPUs, memory, disks, and network adapters of VMs, as well as detailed information about operating systems.<br>● View historical performance of the VM.<br>NOTE<br>Click <b>Performance Threshold Settings</b> on the resource list page to set the monitoring thresholds, including the normal status (in green), risk (in orange), and high risk (in red) for indicators such as CPU utilization and memory utilization.</td><td>1. Choose <b>Resource</b> > <b>Virtual Resources</b> from the main menu.<br>2. Choose <b>Virtual Resources</b> > <b>FusionCompute</b> in the navigation area on the left.<br>3. Click the name of a FusionCompute to access its resource manager.<br>4. Choose <b>Computing Resources</b> > <b>Virtual Machines</b> in the navigation area on the left.<br>5. Click the name of a VM to access its resource manager.</td></tr>
</table>
eSight Operations Guide Issue 08 (2018-08-28) at 982-83.
</td></tr>
</table>

| '227 PATENT CLAIM 3 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| |  |

| Task Name | Task Description | Operation Entry |
|---|---|---|
| Viewing host information | ● View the statuses, IP addresses, CPU usage, memory usage, and routes of hosts.<br>● View the status of all VMs in hosts.<br>● View the list of all VMs in hosts.<br>● View historical performance of the hosts.<br>NOTE<br>Click **Performance Threshold Settings** on the resource list page to set the monitoring thresholds, including the normal status (in green), risk (in orange), and high risk (in red) for indicators such as CPU utilization and memory utilization. | 1. Choose **Resource** > **Virtual Resources** from the main menu.<br>2. Choose **Virtual Resources** > **vCenter Server** in the navigation area on the left.<br>3. Click the name of a vCenter server to access its resource manager.<br>4. Choose **Computing Resources** > **Hosts** in the navigation area on the left.<br>5. Click the name of a host to access its resource manager. |

<table>
<tr><th>'227 PATENT CLAIM 3</th><th>INFRINGEMENT BY HUAWEI CORPORATION</th></tr>
<tr><td></td><td>

<table>
<tr><th>Task Name</th><th>Task Description</th><th>Operation Entry</th></tr>
<tr><td>Viewing VM information</td><td>● View VM information, including VM status, IP address, homed host, and operating system.<br>● View the statistics of key performance counters of VMs, including CPU usage, memory usage, and network adapter rate.<br>● View the resource usage of all VMs on a host to adjust resource allocation in time.<br>● View network traffic analysis data.<br>NOTE<br>Network traffic analysis data is provided only for VMs bound with EIP.<br>● View detailed configurations of CPUs, memory, disks, and network adapters of VMs, as well as detailed information about operating systems.<br>● View historical performance of the VM.<br>NOTE<br>Click <b>Performance Threshold Settings</b> on the resource list page to set the monitoring thresholds, including the normal status (in green), risk (in orange), and high risk (in red) for indicators such as CPU utilization and memory utilization.</td><td>● Method one:<br>1. Choose <b>Resource</b> > <b>Virtual Resources</b> from the main menu.<br>2. Choose <b>Virtual Resources</b> > <b>vCenter Server</b> in the navigation area on the left.<br>3. Click the name of a vCenter server to access its resource manager.<br>4. Choose <b>Computing Resources</b> > <b>Virtual Machines</b> in the navigation area on the left.<br>5. Click the name of a VM to access its resource manager.<br>● Method Two:<br>1. Click the <b>Search</b> icon in the upper right corner and set search criteria, for example, the name of a VM.<br>2. Select the VM you want to view and click it to access the VM resource manager.</td></tr>
</table>
eSight Operations Guide Issue 08 (2018-08-28) at 997-998.</td></tr>
</table>

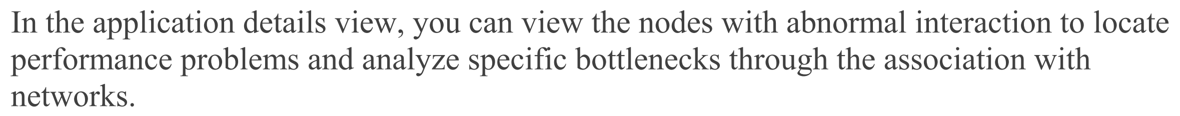
| '227 PATENT CLAIM 3 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|

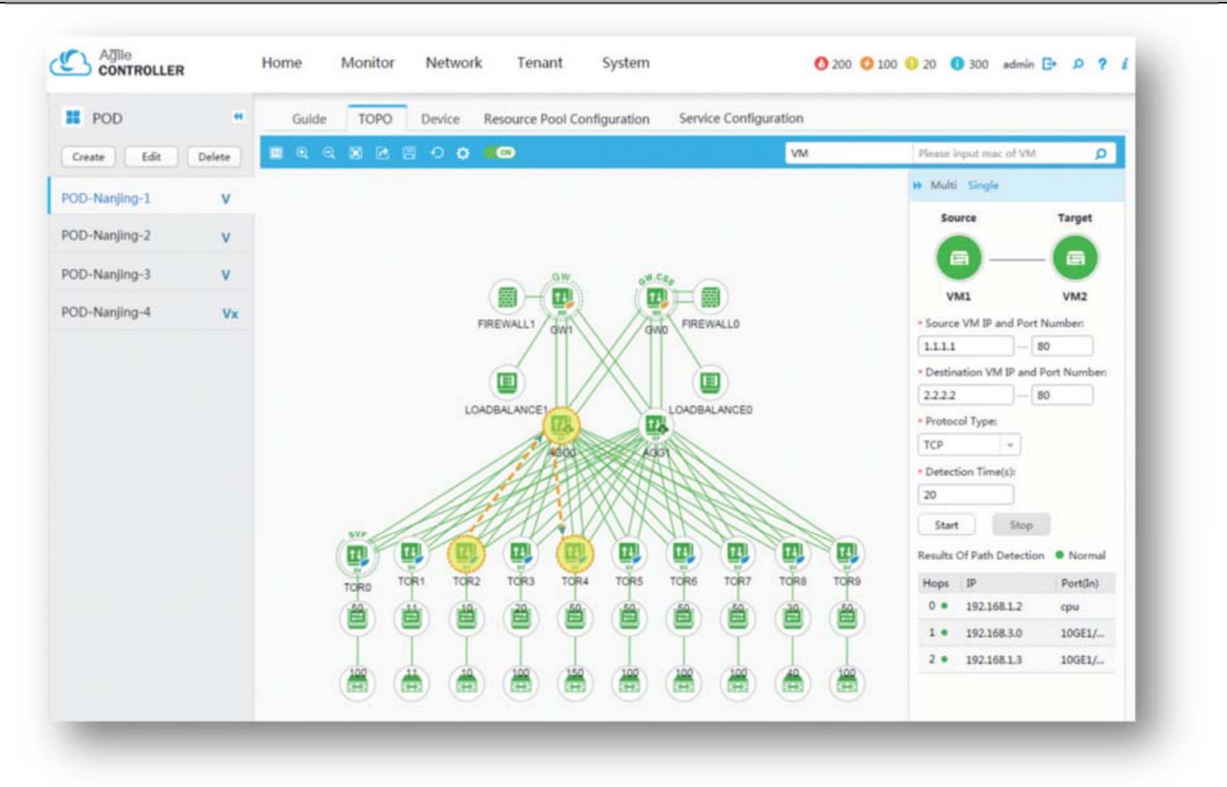


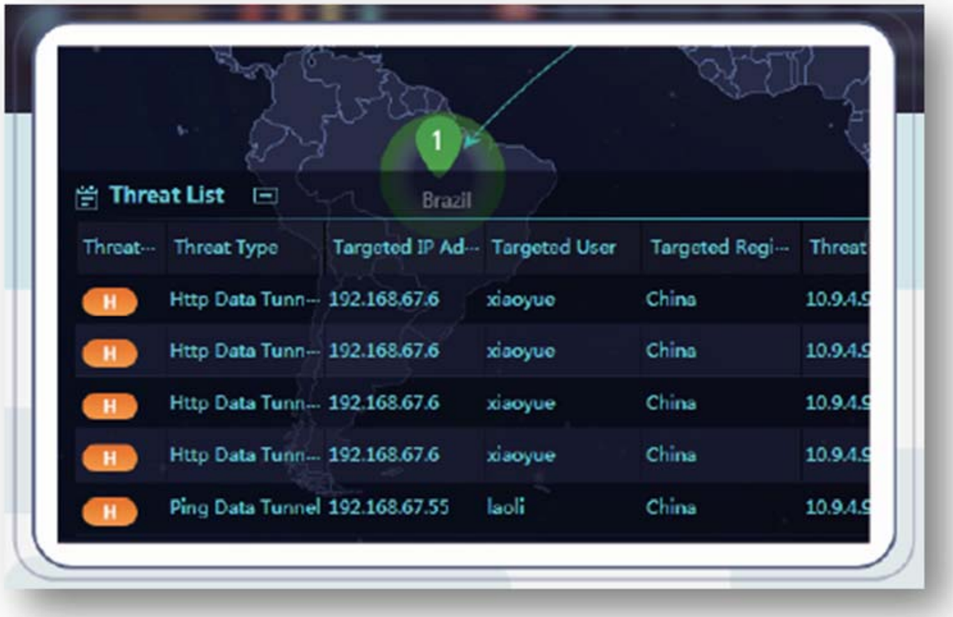
| Task Name | Task Description | Operation Entry |
|---|---|---|
| Viewing host information | ● View the running status, business IP addresses, and total CPU usage of hosts.<br>● View the list of all VMs in hosts.<br>NOTE:<br>Click **Performance Threshold Settings** on the resource list page to set the monitoring thresholds, including the normal status (in green), risk (in orange), and high risk (in red) for indicators such as CPU utilization and memory utilization. | 1. Choose **Resource** > **Virtual Resources** from the main menu.<br>2. Choose **Virtual Resources** > **RedHat Openstack** in the navigation area on the left.<br>3. Click the name of a RedHat Openstack to access its resource manager.<br>4. Choose **Computing Resources** > **Hosts** in the navigation area on the left.<br>5. Click the name of a host to access its resource manager. |
| Viewing VM information | ● View VM information, including VM status, CPU cores, memory and disk.<br>● View the list of all virtual disks in VMs.<br>NOTE:<br>Click **Performance Threshold Settings** on the resource list page to set the monitoring thresholds, including the normal status (in green), risk (in orange), and high risk (in red) for indicators such as CPU utilization and memory utilization. | 1. Choose **Resource** > **Virtual Resources** from the main menu.<br>2. Choose **Virtual Resources** > **RedHat Openstack** in the navigation area on the left.<br>3. Click the name of a RedHat Openstack to access its resource manager.<br>4. Choose **Computing Resources** > **Virtual Machines** in the navigation area on the left.<br>5. Click the name of a VM to access its resource manager. |

eSight Operations Guide Issue 08 (2018-08-28) at 1014-15.

In FabricInsights, for example, on information and belief, there is a manager window for displaying properties of network elements. See, e.g.,

| ’227 Patent Claim 3 | Infringement By Huawei Corporation |
|---|---|
|  |  In the application details view, you can view the nodes with abnormal interaction to locate performance problems and analyze specific bottlenecks through the association with networks.<br>Huawei FabricInsight Datasheet at 3.<br>In Agile Controller, for example, on information and belief, there is a manager window for displaying properties of network elements. For example, there is a window for “device” |

| '227 PATENT CLAIM 3 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| | <br> Agile CONTROLLER Home Monitor Network Tenant System 200 100 20 300 admin POD Create Edit Delete POD-Nanjing-1 V POD-Nanjing-2 V POD-Nanjing-3 V POD-Nanjing-4 Vx Guide TOPO Device Resource Pool Configuration Service Configuration ON VM Please input mac of VM Multi Single Source Target VM1 VM2 GW GW,CSS FIREWALL1 GW1 GW0 FIREWALL0 LOADBALANCE1 LOADBALANCE0 AGG0 AGG1 TOR0 TOR1 TOR2 TOR3 TOR4 TOR5 TOR6 TOR7 TOR8 TOR9 Start Stop<br>* Source VM IP and Port Number: 1.1.1.1 — 80<br>* Destination VM IP and Port Number: 2.2.2.2 — 80<br>* Protocol Type: TCP<br>* Detection Time(s): 20<br>Results Of Path Detection ● Normal<br>Hops IP Port(In)<br>0 ● 192.168.1.2 cpu<br>1 ● 192.168.3.0 10GE1/...<br>2 ● 192.168.1.3 10GE1/...<br>Huawei Agile Controller 3.0 Brief Brochure V1.0 at 2.<br>In CIS, for example, there is a manager window for displaying properties of network elements. *See e.g.,*:<br>Quick identification of highrisk assets and main threats |

<table>
<tr><th>'227 PATENT<br>CLAIM 3</th><th>INFRINGEMENT BY HUAWEI CORPORATION</th></tr>
<tr><td></td><td>
The CIS visually displays threats that target the internal users and assets of an enterprise, quickly identifies high-risk assets and main threats by categorizing users, asset groups, and threat events, and helps users specify regions to be secured and the solutions.<br>


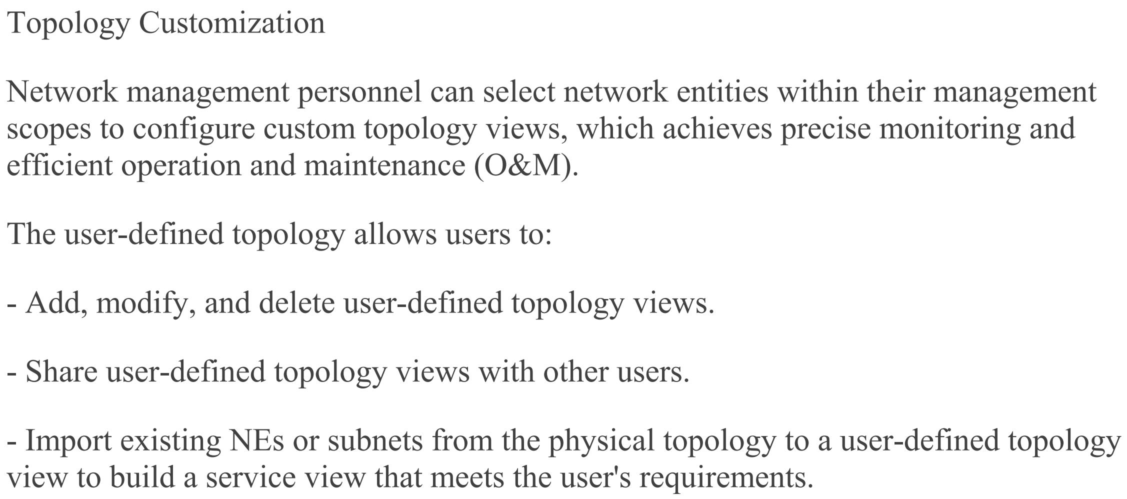
Threat List<br>
<table>
<tr><th>Threat···</th><th>Threat Type</th><th>Targeted IP Ad···</th><th>Targeted User</th><th>Targeted Regi···</th><th>Threat</th></tr>
<tr><td>H</td><td>Http Data Tunn···</td><td>192.168.67.6</td><td>xiaoyue</td><td>China</td><td>10.9.4.9</td></tr>
<tr><td>H</td><td>Http Data Tunn···</td><td>192.168.67.6</td><td>xiaoyue</td><td>China</td><td>10.9.4.9</td></tr>
<tr><td>H</td><td>Http Data Tunn···</td><td>192.168.67.6</td><td>xiaoyue</td><td>China</td><td>10.9.4.9</td></tr>
<tr><td>H</td><td>Http Data Tunn···</td><td>192.168.67.6</td><td>xiaoyue</td><td>China</td><td>10.9.4.9</td></tr>
<tr><td>H</td><td>Ping Data Tunnel</td><td>192.168.67.55</td><td>laoli</td><td>China</td><td>10.9.4.9</td></tr>
</table>
Huawei CIS Cybersecurity Intelligence System Product Description at 3.
</td></tr>
</table>

| **'227 Patent Claim 4** | **Infringement By Huawei Corporation** |
|---|---|
| **4.** A graphical user interface according to claim 1, wherein icons are linked together by arrows that turn a different color indicative of a vulnerable connection that exists between network elements. | The Huawei '227 Patent Accused Instrumentalities infringe this claim. *See* Claim 1.<br>The Accused Instrumentalities further comprise icons that are linked together by arrows that turn a different color indicative of a vulnerable connection that exists between network elements.<br>*See* Claim 1[b] |

| **'227 Patent Claim 5** | **Infringement By Huawei Corporation** |
|---|---|
| **5.** A graphical user interface contained on a computer screen and used for determining the security posture of a network comprising: | The Huawei '227 Patent Accused Instrumentalities infringe this claim.<br>For example, the Accused Instrumentalities contain a graphical user interface on a computer screen that can be used for determining the security posture of a network.<br>*See* Claim 1 [preamble] above. |
| **[a]** a system design window for displaying icons of a network map that are representative of different network nodes contained within a network, wherein respective icons are linked | The Huawei '227 Patent Accused Instrumentalities comprise a system design window for displaying icons of a network map that are representative of different network nodes contained within a network, wherein respective icons are linked together in an arrangement corresponding to how network nodes are interconnected within the network;<br>*See* Claim 1[a] above |

| **'227 PATENT CLAIM 5** | **INFRINGEMENT BY HUAWEI CORPORATION** |
|---|---|
| together in an arrangement corresponding to how network nodes are interconnected within the network; | |
| **[b]** a manager window on which respective properties of network nodes are displayed and edited; | The Huawei '227 Patent Accused Instrumentalities comprise a manager window on which respective properties of network nodes are displayed and edited.<br>*See* Claim 3 above. |
| **[c]** wherein selected icons turn the color red indicative of a higher risk node and selected icons turn yellow indicative of a less severe risk node after a vulnerability posture of the network has been established by correlating a system object model database that supports information data requirements of disparate network vulnerability analysis programs with any data | In the Huawei '227 Patent Accused Instrumentalities selected icons turn the color red indicative of a higher risk node and selected icons turn yellow indicative of a less severe risk node after a vulnerability posture of the network has been established by correlating a system object model database that supports information data requirements of disparate network vulnerability analysis programs with any data results obtained from the programs.<br>*See* Claim 1[b] above. |

| '227 PATENT CLAIM 5 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| results obtained from the programs. | |

| '227 PATENT CLAIM 6 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| **6.** A graphical user interface according to claim 5, wherein said manager window further comprises a node properties display box for editing the properties of network nodes for network design alternatives. | The Huawei '227 Patent Accused Instrumentalities infringe this claim. *See* Claim 5.<br>Further, a manager window further comprises a node properties display box for editing the properties of network nodes for network design alternatives.<br>For example, in eSight, users may customize the topology for network design alternatives:<br><br>Topology Customization<br>Network management personnel can select network entities within their management scopes to configure custom topology views, which achieves precise monitoring and efficient operation and maintenance (O&M).<br>The user-defined topology allows users to:<br>- Add, modify, and delete user-defined topology views.<br>- Share user-defined topology views with other users.<br>- Import existing NEs or subnets from the physical topology to a user-defined topology view to build a service view that meets the user's requirements. |

| '227 PATENT CLAIM 6 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
|  | - Adjust the existing members in a user-defined topology view.<br>eSight Operations Guide Issue 08 (2018-08-28) at 295.<br>Further, on information and belief, FabricInsights, Agile Controller and CIS further comprise a node properties display box for editing the properties of network nodes for network design alternatives. For example:<br>Based on Huawei SDN controller—the Agile Controller—drag-and-drop deployment can be achieved. The Agile Controller automatically forwards network design models as configurations to be deployed on the physical network, implementing service provisioning in minutes.<br>CloudFabric Data Center Network Solution Brochure at 11. |

| '227 PATENT CLAIM 8 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| **8.** A graphical user interface according to claim 5, and further comprising a select node configuration edit box having a user selectable vulnerability profile for selecting a vulnerability of a respective node. | The Huawei '227 Patent Accused Instrumentalities infringe this claim. *See* Claim 5.<br>Further, the GUI comprises a select node configuration edit box having a user selectable vulnerability profile for selecting a vulnerability of a respective node.<br>In a non-limiting example, user-defined alarm thresholds may be configured that allow a user to select a vulnerability of a node.<br>*See* Claim 1[b] |

| '227 PATENT<br>CLAIM 9 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| **9.** A graphical user interface contained on a computer screen and used for determining the security posture of a network comprising: | The Huawei '227 Patent Accused Instrumentalities infringe this claim.<br>For example, the Accused Instrumentalities contain a graphical user interface on a computer screen that can be used for determining the security posture of a network.<br>*See* Claim 1 [preamble] above. |
| **[a]** a system design window for displaying network icons of a network map that are representative of different network elements contained within a network, wherein respective network icons are linked together in an arrangement corresponding to how network elements are interconnected within the network, wherein selected portions of the network map turn a different color indicative of a vulnerability that has been established for that portion of the network after a security posture of the network has been established by correlating a system object | The Huawei '227 Patent Accused Instrumentalities comprise a system design window for displaying network icons of a network map that are representative of different network elements contained within a network, wherein respective network icons are linked together in an arrangement corresponding to how network elements are interconnected within the network, wherein selected portions of the network map turn a different color indicative of a vulnerability that has been established for that portion of the network after a security posture of the network has been established by correlating a system object model database that supports information data requirements of disparate network vulnerability analysis programs with any data results obtained from the programs.<br>*See* Claim 1[a] and 1[b] above. |

| '227 Patent Claim 9 | Infringement By Huawei Corporation |
|---|---|
| model database that supports information data requirements of disparate network vulnerability analysis programs with any data results obtained from the programs; and | |
| **[b]** a vulnerability posture window for displaying user readable items indicative of vulnerable network elements. | The Huawei '227 Patent Accused Instrumentalities comprise a vulnerability posture window for displaying user readable items indicative of vulnerable network elements.<br>For example, a user may view readable items that indicate vulnerable network elements, including, for example, user-defined alarm thresholds that may be configured by the user. Further, a user may view alarms which may be indicative of a vulnerable network element.<br>*See* Claim 1[b] |

| '227 Patent Claim 10 | Infringement By Huawei Corporation |
|---|---|
| **10.** A graphical user interface according to claim 9, wherein said user readable items comprise a chart indicative of | The Huawei '227 Patent Accused Instrumentalities infringe this claim. *See* Claim 9.<br>Further, user readable items comprise a chart indicative of vulnerable network elements.<br>For example, in eSight, alarms that may indicate vulnerable network elements may be viewed in a chart: |

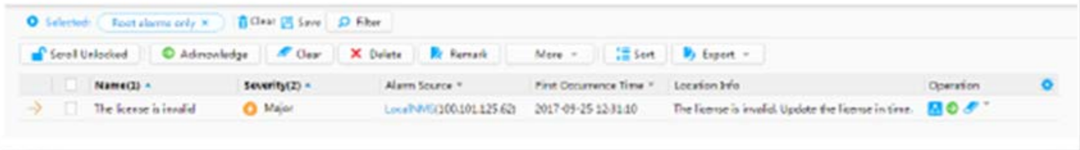
<table>
<tr><th>'227 PATENT CLAIM 10</th><th>INFRINGEMENT BY HUAWEI CORPORATION</th></tr>
<tr><td>vulnerable network elements.</td><td>

Alarm Monitoring

The eSight provides various alarm monitoring methods and multidimensional alarm data statistics.

- Monitor alarms in the current alarm list.

Figure 5-1 Current alarms



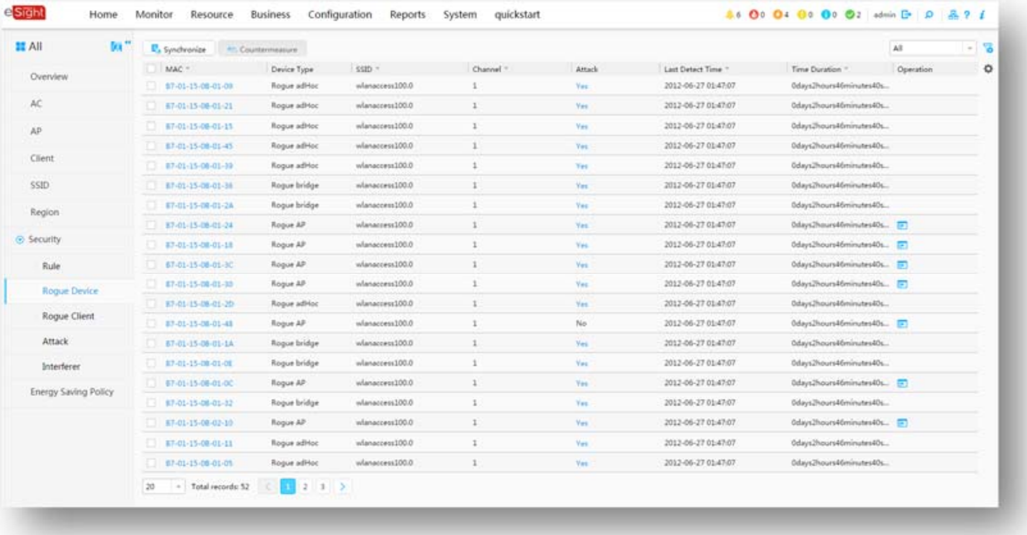
<table>
<tr><th>Name(1)</th><th>Severity(2)</th><th>Alarm Source</th><th>First Occurrence Time</th><th>Location Info</th></tr>
<tr><td>The license is invalid</td><td>Major</td><td>LocalNMS(100.101.125.62)</td><td>2017-09-25 12:31:10</td><td>The license is invalid. Update the license in time.</td></tr>
</table>

eSight Operations Guide Issue 08 (2018-08-28) at 213.

*See also, e.g.,*

</td></tr>
</table>

| ’227 PATENT CLAIM 10 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|

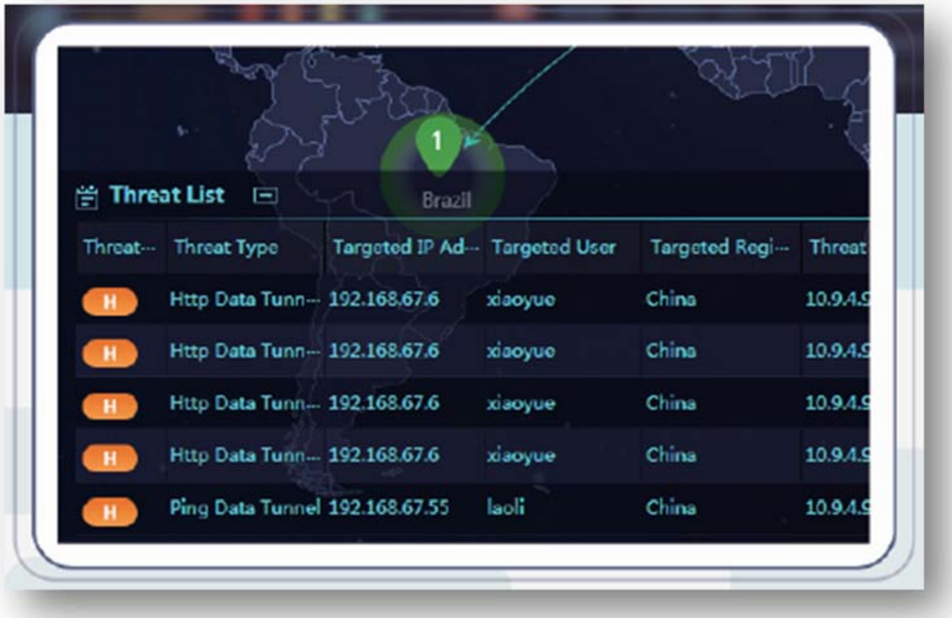


| MAC | Device Type | SSID | Channel | Attack | Last Detect Time | Time Duration | Operation |
|---|---|---|---|---|---|---|---|
| 87-01-15-08-01-09 | Rogue adHoc | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| 87-01-15-08-01-21 | Rogue adHoc | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| 87-01-15-08-01-15 | Rogue adHoc | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| 87-01-15-08-01-45 | Rogue adHoc | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| 87-01-15-08-01-39 | Rogue adHoc | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| 87-01-15-08-01-38 | Rogue bridge | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| 87-01-15-08-01-2A | Rogue bridge | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| 87-01-15-08-01-24 | Rogue AP | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | ▤ |
| 87-01-15-08-01-18 | Rogue AP | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | ▤ |
| 87-01-15-08-01-3C | Rogue AP | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | ▤ |
| 87-01-15-08-01-30 | Rogue AP | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | ▤ |
| 87-01-15-08-01-2D | Rogue adHoc | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| 87-01-15-08-01-48 | Rogue AP | wlanaccess100.0 | 1 | No | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | ▤ |
| 87-01-15-08-01-1A | Rogue bridge | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| 87-01-15-08-01-0E | Rogue bridge | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| 87-01-15-08-01-0C | Rogue AP | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | ▤ |
| 87-01-15-08-01-32 | Rogue bridge | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| 87-01-15-08-02-10 | Rogue AP | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | ▤ |
| 87-01-15-08-01-11 | Rogue adHoc | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |
| 87-01-15-08-01-05 | Rogue adHoc | wlanaccess100.0 | 1 | Yes | 2012-06-27 01:47:07 | 0days2hours46minutes40s... | |

20 Total records: 52 1 2 3

HUAWEI eSight WLAN White Paper Issue 01 (2017-03-20) at 10 (see also, charts showing additional vulnerable network elements at p. 11).

The CIS user interface further comprises a chart indicative of vulnerable network elements, for example:

<table>
<tr><th>'227 PATENT<br>CLAIM 10</th><th>INFRINGEMENT BY HUAWEI CORPORATION</th></tr>
<tr><td></td><td>


Threat List
<table>
<tr><th>Threat···</th><th>Threat Type</th><th>Targeted IP Ad···</th><th>Targeted User</th><th>Targeted Regi···</th><th>Threat</th></tr>
<tr><td>H</td><td>Http Data Tunn···</td><td>192.168.67.6</td><td>xiaoyue</td><td>China</td><td>10.9.4.9</td></tr>
<tr><td>H</td><td>Http Data Tunn···</td><td>192.168.67.6</td><td>xiaoyue</td><td>China</td><td>10.9.4.9</td></tr>
<tr><td>H</td><td>Http Data Tunn···</td><td>192.168.67.6</td><td>xiaoyue</td><td>China</td><td>10.9.4.9</td></tr>
<tr><td>H</td><td>Http Data Tunn···</td><td>192.168.67.6</td><td>xiaoyue</td><td>China</td><td>10.9.4.9</td></tr>
<tr><td>H</td><td>Ping Data Tunnel</td><td>192.168.67.55</td><td>laoli</td><td>China</td><td>10.9.4.9</td></tr>
</table>
Huawei CIS Cybersecurity Intelligence System Product Description at 3.<br>On information and belief, the GUI of the other Accused Instrumentalities contain similar functionality.
</td></tr>
</table>

| '227 PATENT CLAIM 11 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| **11.** A graphical user interface according to claim 9, wherein said user readable items comprise a spreadsheet indicating the vulnerable network elements. | The Huawei '227 Patent Accused Instrumentalities infringe this claim. *See* Claim 9.<br>Further, user readable items comprise a spreadsheet indicating the vulnerable network elements.<br>For example, in eSight, unauthorized access reports are sent via Excel, indicating vulnerable network elements:<br>12.3.4.1 Example for Using Terminal Resource Management to Monitor<br>Unauthorized Users<br>This example illustrates how enterprise administrators use eSight to discover unauthorized terminals in a timely and effective manner, to ensure network stability and security.<br>…<br>After the preceding settings are complete, eSight will send new unauthorized access information (in Excel format) to Jack by emails, so Jack can obtain unauthorized access information in a timely manner.<br>eSight Operations Guide Issue 08 (2018-08-28) at 1121-1126.<br>On information and belief, the GUI of the other Accused Instrumentalities contain similar functionality. |

| '227 PATENT CLAIM 12 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| **12.** A graphical user interface according to claim 9, wherein respective network elements represented by icons turn a different color indicative of a vulnerable network node. | The Huawei '227 Patent Accused Instrumentalities infringe this claim. *See* Claim 9.<br>Further, respective network elements represented by icons turn a different color indicative of a vulnerable network node.<br>*See* Claims 1[b] and 2. |

| '227 PATENT CLAIM 13 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| **13.** A graphical user interface according to claim 9, and further comprising a manager window for displaying properties of network elements. | The Huawei '227 Patent Accused Instrumentalities infringe this claim. *See* Claim 9.<br>The Accused Instrumentalities further comprise a manager window for displaying properties of network elements.<br>*See* Claim 3. |

| '227 PATENT CLAIM 15 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| **15.** A graphical user interface according to claim 9, and further comprising a select node configuration edit box having a user selectable | The Huawei '227 Patent Accused Instrumentalities infringe this claim. *See* Claim 9.<br>The Accused Instrumentalities further comprise a select node configuration edit box having a user selectable vulnerability profile for a network node. |

| '227 PATENT CLAIM 15 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| vulnerability profile for a network node. | *See* Claims 1[b] and 8. |

| '227 PATENT CLAIM 16 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| **16.** A graphical user interface according to claim 9, wherein icons are linked together by arrows that turn a different color indicative of a vulnerable connection that exists between network elements. | The Huawei '227 Patent Accused Instrumentalities infringe this claim. *See* Claim 9.<br>Further, icons are linked together by arrows that turn a different color indicative of a vulnerable connection that exists between network elements.<br>*See* Claim 1[b] |

| '227 PATENT CLAIM 17 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| **17.** A graphical user interface contained on a computer screen and used for determining the security posture of a network comprising: | The Huawei '227 Patent Accused Instrumentalities infringe this claim.<br>For example, the Accused Instrumentalities comprise a graphical user interface on a computer screen that can be used for determining the security posture of a network.<br>*See* Claim 1 [preamble] above. |

| '227 Patent Claim 17 | Infringement By Huawei Corporation |
|---|---|
| **[a]** a system design window for displaying icons of a network map that are representative of different network nodes contained within a network, wherein respective icons are linked together in an arrangement corresponding to how the network nodes are interconnected within the network; | The Huawei '227 Patent Accused Instrumentalities comprise a system design window for displaying icons of a network map that are representative of different network nodes contained within a network, wherein respective icons are linked together in an arrangement corresponding to how the network nodes are interconnected within the network.<br>*See* Claim 1[a] |
| **[b]** a manager window on which respective properties of network nodes are displayed and edited; | The Huawei '227 Patent Accused Instrumentalities comprise a manager window on which respective properties of network nodes are displayed and edited.<br>*See* Claim 3 above. |
| **[c]** wherein selected icons turn the color red indicative of a higher risk node and selected icons turn yellow indicative of a less severe risk node after a security posture of the network has been established by correlating a | In the Huawei '227 Patent Accused Instrumentalities selected icons turn the color red indicative of a higher risk node and selected icons turn yellow indicative of a less severe risk node after a security posture of the network has been established by correlating a system object model database that supports information data requirements of disparate network vulnerability analysis programs, with any data results obtained from the programs.<br>*See* Claim 1[b]. |

| '227 PATENT CLAIM 17 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| system object model database that supports information data requirements of disparate network vulnerability analysis programs, with any data results obtained from the programs; and | |
| **[d]** a vulnerability posture window for displaying user readable items indicative of vulnerable network icons. | The Huawei '227 Patent Accused Instrumentalities comprise a vulnerability posture window for displaying user readable items indicative of vulnerable network icons.<br>*See* Claim 1[b]. |

| '227 PATENT CLAIM 18 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| **18.** A graphical user interface according to claim 17, wherein said user readable items comprise a chart indicative of vulnerable network nodes. | The Huawei '227 Patent Accused Instrumentalities infringe this claim. *See* Claim 17.<br>Further, said user readable items comprise a chart indicative of vulnerable network nodes.<br>*See* Claim 10. |

| '227 PATENT CLAIM 19 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| **19.** A graphical user interface according to claim 17, wherein said user readable items comprise a spreadsheet indicating the vulnerable network nodes. | The Huawei '227 Patent Accused Instrumentalities infringe this claim. *See* Claim 17.<br>Further, said user readable items comprise a spreadsheet indicating the vulnerable network nodes.<br>*See* Claim 11. |

| '227 PATENT CLAIM 20 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| **20.** A graphical user interface according to claim 17, wherein said manager window further comprises a node properties display box for editing the properties of network nodes for network design alternatives. | The Huawei '227 Patent Accused Instrumentalities infringe this claim. *See* Claim 17.<br>Further, said manager window further comprises a node properties display box for editing the properties of network nodes for network design alternatives.<br>*See* Claim 6. |

| '227 PATENT CLAIM 22 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| **22.** A graphical user interface according to claim 17, and further comprising a select | The Huawei '227 Patent Accused Instrumentalities infringe this claim. *See* Claim 17. |

| '227 PATENT CLAIM 22 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| node configuration edit box having a user selectable vulnerability profile for a respective node. | The Accused Instrumentalities further comprise a select node configuration edit box having a user selectable vulnerability profile for a respective node.<br>*See* Claims 1[b] and 8 |

| '227 PATENT CLAIM 24 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| **24.** A graphical user interface contained on a computer screen and used for determining the security posture of a network comprising: | The Huawei '227 Patent Accused Instrumentalities infringe this claim.<br>For example, the Accused Instrumentalities have a graphical user interface contained on a computer screen that can be used for determining the security posture of a network.<br>*See* Claim 1 [preamble] above. |
| **[a]** a system design window for displaying network icons of a network map that are representative of different network elements contained within a network, wherein respective network icons are linked together in an arrangement corresponding to how network elements are interconnected within the | The Huawei '227 Patent Accused Instrumentalities comprise a system design window for displaying network icons of a network map that are representative of different network elements contained within a network, wherein respective network icons are linked together in an arrangement corresponding to how network elements are interconnected within the network and a select node configuration edit box having a user selectable vulnerability profile for selecting a vulnerability profile of a network node.<br>*See* Claims 1[a], 1[b] and 8. |

| '227 PATENT<br>CLAIM 24 | INFRINGEMENT BY HUAWEI CORPORATION |
|---|---|
| network and a select node configuration edit box having a user selectable vulnerability profile for selecting a vulnerability profile of a network node; | |
| **[b]** wherein selected portions of the network map turn a different color indicative of a vulnerability that has been established for that portion of the network after a security posture of the network has been established. | The graphical user interface of the '227 Patent Accused Instrumentalities further comprises the capability for selected portions of the network map to turn a different color indicative of a vulnerability that has been established for that portion of the network after a security posture of the network has been established.<br>*See* Claim 1[b]. |